BREAKING DOWN DIGITAL BARRIERS

CASE STUDY

Digital Identity Interoperability and eInnovation

by John Palfrey *and* Urs Gasser

Berkman
The Berkman Center for Internet & Society
at Harvard Law School

Research Center
for Information Law
University of St.Gallen

Sponsored by:
Microsoft

CASE STUDY

Digital Identity Interoperability and eInnovation

John Palfrey *and* Urs Gasser

Berkman Publication Series, November 2007
http://cyber.law.harvard.edu/interop

The Berkman Center for Internet & Society, Harvard University
Research Center for Information Law, University of St. Gallen
Sponsored by Microsoft®

This work is licensed under the Creative Commons
Attribution-Noncommercial-Share Alike 3.0 United States License.
To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/3.0/us/

TABLE OF CONTENTS

INTRODUCTION

The Internet was not built with embedded security and privacy infrastructures. Instead, its framers favored a "procrastination principle"[1] of allowing others to develop these features as they were needed, and then, specific to a particular application rather than network-wide. In large part because of the flexibility of a network that does not have extensive security and privacy frameworks, the Internet is now used by over a billion people worldwide.[2] E-commerce is a major component of Internet use, with $31.5 billion in U.S. retail sales over the Internet in the first quarter of 2007.[3] Sales topped £10 billion in the first quarter of 2007 in the United Kingdom.[4] Online banking customers increased to 53 million in the U.S. in 2005, including 44% of Internet users at that time.[5] In Australia, 68% of Internet users bank online at least once a week.[6] Thirteen million Americans made donations online after Hurricanes Katrina and Rita in 2005,[7] and half of all American donations to the 2005 Tsunami relief effort were made online.[8] The upsweep of non-profit organizations' presence online allows for greater online giving, from making donations to traditional organizations to using innovative online-loan sites such as prosper.com and microfinance site kiva.org.

[1] Jonathan Zittrain, The Future of the Internet – and How to Stop It (forthcoming, Yale University Press, 2008).

[2] CIA World Factbook, Internet Users Ranked by Country, https://www.cia.gov/library/publications/the-world-factbook/rankorder/2153rank.html (last updated 18 October 2007).

[3] U.S. Census Bureau Department of Commerce, Quarterly Retail E-Commerce Sales: 1st Quarter 2007, Press Release, May 16, 2007, http://www.census.gov/mrts/www/data/html/07Q1.html.

[4] Extrapolated from Tash Shifrin, UK online shopping sales hit £100 billion mark, May 21, 2007, http://www.macworld.co.uk/news/index.cfm?RSS&newsID=18080.

[5] Online Banking 2005: A Pew Internet Project Data Memo, February 8, 2005, http://www.pewinternet.org/PPF/r/149/report_display.asp.

[6] AC Nielsen, Aussie consumers choose Internet banking over ATM, phone and branch, April 26, 2007, http://au.acnielsen.com/site/InternetBanking.shtml.

[7] Stephen Morris and John Horrigan, 13 million Americans made donations online after Hurricanes Katrina and Rita, November 24, 2005, http://www.pewinternet.org/PPF/r/168/report_display.asp.

[8] Bill Clinton, speech to the Harvard University class of 2007, June 3, 2007, available at http://www.news.harvard.edu/gazette/2007/06.14/99-gates.html.

E-commerce is, of course, only the most prominent part of a story that implicates security and privacy. Facebook, a leading social networking site, had 34 million users as of August 2007, with 200,000 new users joining each day. At this rate, there will be well over 60 million Facebook users by the end of 2007.[9] Increasingly, individuals rely on the Internet as a vehicle for receiving news – in one study, 19% of people aged 18-24 from around the world saw the Internet as the most important source of news.[10] As we move more of our lives online, issues surrounding identity and identification online become more complex, and more important – yet our methods of assuring identity remain uneven and application-specific.

The extent to which so many daily activities are now carried out over the Internet has introduced an emerging set of concerns over one's digital identity. Every time we enter credit card information into a Web site to make a purchase, type in our demographic details or music preferences, or log in to a Web site to book travel arrangements, we are divulging personal information. Such personal information is usually kept solely by the services we use and is not transferable from one service to another. While this can prevent a "Fort Knox" problem, in which the compromise of one's identity affects all of one's Internet activities because one repository contains all of one's identifying information, there is a corresponding problem of managing and safeguarding one's identity across disparate applications and uses.

Because identity is managed one application at a time, the Internet allows ample space for anonymity and pseudonymity. A given application need only refrain from requesting and authenticating identifying information from its users to enable users to remain either anonymous or pseudonymous. In many cases, this anonymity empowers users and inspires them to share new ideas. At the same time, the ability to verify one's identity on the Internet, or at least to establish persistent pseudonyms that can achieve reputation in repeat transactions, is essential for certain online exchanges. These activities include

[9] See Nicole Maestri, Wal-Mart using Facebook to win back-to-school sales, August 8, 2007, http://www.reuters.com/article/businessNews/idUSN0843464220070809; see also Facebook Statistics, http://www.facebook.com/press/info.php?statistics (last visited 5 November 2007).

[10] Research firm Globespan questioned 10,000 people in the UK, US, Brazil, Egypt, Germany, India, Indonesia, Nigeria, Russia, and South Korea between March and April 2006. See Alfred Hermida, Young challenge mainstream media, May 3, 2006, http://news.bbc.co.uk/2/hi/technology/4962794.stm.

buying, selling, banking, participating in certain community groups, and collaborating on projects. Individuals' ability to accurately and easily share identifying information about themselves – and learn that of others – is key to the continued transactional success of the Internet.

The absence of such verified identity is a challenge for basic applications such as email, where we often cannot be certain with whom we are communicating. The question of how best to share or ascertain necessary identifying information securely while protecting users' privacy has come to the fore. This question has intrigued major players in technology, and it has begun to bring many of them together in collaboration.

The services we use today are cobbled together and insecure partly because of a lack of good methods for authentication and accreditation. These shortcomings have precluded certain types of innovation that might have occurred were these capabilities in existence. A major question in addressing these problems is that of interoperability: the ability to maintain an interconnected identity framework that permits credentials from one application to be readily honored by another.

This case study addresses the issue of Digital ID interoperability, specifically in the Internet context. First, we undertake to define Digital ID interoperability by specifying some of its attributes, thereby arriving at a working definition. In Part 1.2, we consider experiences in creating Digital ID interoperability to date and in Part 1.3, we look at some of the forces that drive or inhibit the emergence of interoperability in Digital ID. In Part 2, we assess the benefits and drawbacks of Digital ID interoperability as they relate to innovation, and in Part 3 we discuss some potential paths forward. We find that while mechanisms for technical interoperability have been developed, there remain significant additional barriers to interoperability. In particular, the continued ability and willingness of relevant people and companies to work together on technology and marketing will be crucial to the uptake of an interoperable Digital ID system. Such interoperability will most likely spur innovation as widely used Digital ID solutions enable new applications, as long as issues such as privacy and security will have to be adequately addressed.

1 STATE OF PLAY: DIGITAL ID INTEROPERABILITY

1.1 What is Digital ID Interoperability?

A definition of “Digital ID Interoperability” relies on a definition of “Digital ID,” which is more abstract than personal identity, and as such is more difficult to describe. Identity begins with an assertion (explicit or implicit) that one is a certain person or has a certain characteristic, and is not someone else with other characteristics (authentication). It is relational, including that which a person says about herself and that which others say about that person (reputation or accreditation).[11] In person, authentication begins with visual and auditory cues: a human being walks into a physical place with a certain gait, wearing distinctive clothing, speaking a given language, and so forth. In some circumstances, this self-identification is sufficient; a bald man with a gray beard is unlikely to be asked for government ID to verify age when buying alcohol. Sometimes one’s identity must be further established by reference to accreditation by third parties. In the modern world, the party that performs the verification of one’s identity (say a department of motor vehicles) is often split from the party relying on that identification (say a liquor store). The verification process is accomplished by providing some kind of credential, which the relying party views and determines whether to trust. The storage and use

[11] Dick Hardt, OSCON 2005 Keynote – Identity 2.0, August 1, 2005, http://www.identity20.com/media/OSCON2005/ (“Identity is what I say about me, and what others say about me.”).

of that credential is controlled by the individual, the one in possession of her driver's license. In most cases the liquor store does not retain any information about the individual – they simply check the credential and move on.

Digital ID is a necessary foundation of many forms of online exchange. Online, when users want to engage in an exchange that requires knowing with whom they are dealing, the cues that individuals rely on in the real world are not present. The most common method of accrediting identity online is to use financial institutions, which must have in-person relationships with their clients, as intermediaries, but this only allows validation of a narrow set of personal data, such as credit card numbers and perhaps billing addresses. The exchange of payment information is only a limited example of what we refer to as Digital ID. According to the Identity Gang, a collaborative group of thinkers loosely joined online, Digital ID is defined as "A digital representation of a set of claims made by one party about itself or another digital subject."[12] As Digital ID consists only of a set of claims about an identity, it is simply a bundle of data, less tied to the individual than a personal identity. In this case study, we focus on Digital ID applications between different entities over the Internet; because of the broad, global scope of our inquiry, we wish to point out that we are not primarily addressing identity provisioning within an enterprise when we refer to Digital ID.

A Digital ID system can serve any of several functions: authentication, verification, uniqueness, linkage, and reputation. Identification in general is the process of evaluating – based on the data provided – who a given person is, while "authentication implies that a decision is made based on the actual corroboration of information, implying a larger degree of dependability."[13] Authentication is the verification of the data – or credentials – provided during a user's attempt to gain authorization to do something online. Authorization is granted, in a system of this sort, only after successful authentication. Linkage and reputation are both functions of Digital ID that describe connections – between people, and in what light they view each other.

[12] Identity Gang, Definitions, http://www.identitygang.org/moin.cgi/Identipedia (last visited 30 October 2007).

[13] A Roadmap for a Pan-European eIDM Framework by 2010, http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf (last visited 30 October 2007).

It is important to note that in this case we are focusing on the part of identity that consists of facts about a person; we are not discussing an individual's personality-inspired identity – measured by likes and dislikes, friends, and beliefs--but rather the bundle of data that uniquely distinguishes the individual from all others. The credentials we concern ourselves with here include government-issued ID numbers, credit card information, address, birth date, credit history, etc. This part of one's identity is much more about the various "puzzle pieces" that make you *you* and not someone else, as opposed to the more qualitative elements that comprise one's persona online, increasingly expressed through channels such as MySpace, blogs, and personal Web sites.

Gathering Digital ID information is a challenge. A Web site can gather certain information about a user – such as IP address and client software – passively, but must ask or require the user to actively share any more personally identifying information. The site, ordinarily governed by a private party other than the individual, controls the information – how it is stored and how it is used. While a site's owners request information and it is often in the user's best interest to be truthful and in the site owner's interest to be prudent with the user's data, obtaining and maintaining that information is not a simple task. The mere display of a "registration page" – on which a site asks the user for the information the site deems necessary and relevant to a transaction – is sufficient to cause many users to click away. Most users are tired of filling in forms.[14] If they do register, band-aid techniques are required in order to verify that the people creating the profiles are real. For example, the user account creation process on many Web sites includes a process by which the user enters an email address, the site sends an email to that address with a link or verification code, and the user must click the link or enter the code before her account is activated. This provides some degree of assurance that the user is indeed a live being and not a spambot, and is often sufficient authentication for the site. However, if the site needs to know that the person using it now is the same person who used it yesterday, more ad-hoc authentication is needed. This usually comes in the form of a username and password specific to that site, so, say, a message board will know that it is the same live being commenting yesterday and today, and conversations can be tracked, reputations established, and trust networks built.

[14] Paul Madsen, The Liberty Alliance, April 1, 2003, http://webservices.xml.com/pub/a/ws/2003/04/01/liberty.html.

When users have many profiles, usernames and passwords become cumbersome. The average technology worker spends 14 minutes each day simply logging into and out of the many systems she uses.[15] The problem with the current state of network identity is that the burden of maintaining these islands of identity falls to the individual, who is ill equipped to do so efficiently. It is the individual who is responsible for remembering the multiple user name/ password pairs for each of these user profiles, and it is the individual who must manage the information that each Web site maintains in order to ensure that it is both up to date and appropriate. To address the task of remembering all their user names and passwords, users will typically either try to use the same combination (which isn't always possible) or record these values elsewhere. Either case results in a reduction in the level of security that the user names and passwords were designed to provide. In addition, the ad-hoc nature of creating separate identifying profiles at every Web site makes it difficult for businesses to share information that would be useful for the consumer to have them know. For example, it would be convenient for a travel booking site to know that a user prefers to rent cars from a specific rental company, and to know with what companies the user has rewards cards, without the user having to fill them in if she finds a cheaper rate from a new service. Some Web sites are able to collect this sort of information, but only after the user trusts them with her login information for other sites that have it stored.

Digital identity solutions have been under consideration – and in development – for many years. Smart cards were an early source of authentication, valued for their strength over the username/password mechanism. Smart cards are a type of hardware token,[16] equipped with a computer chip that contains vital information about the cardholder. The card, about the size of a credit card, works when it is read by a card reader, whose software communicates with the chip and carries out certain commands or operations. Most smart cards understand commands written according to ISO 7816 specifications.[17]

[15] Interview with Brian Arbogast, June 4, 2007.

[16] Hardware tokens are physical objects that, usually in conjunction with a password or other security measure, serve to authenticate the holder and allow access to a secure system. We recognize that numerous types of hardware tokens are in use, but only treat smart cards here to simplify the discussion. Many of the same issues apply to other hardware tokens as well.

[17] Wikipedia, Smart card, http://en.wikipedia.org/wiki/Smart_card (last visited 30 October 2007).

Not all smart cards are interoperable, though, and their design has a range of drawbacks and limitations.[18] Two U.S. government agencies, the General Services Administration (GSA) and the National Institute of Standards and Technology (NIST) have only recently begun thinking about a standardized interface that would allow all types of smart cards (and there are at least 100 varieties) to communicate with each other.[19]

Digital certificates, another security mechanism for digital identification, have been in use for decades in one form or another.[20] Digital certificates are attachments to email or other communications intended to ensure that the sender is indeed the person he or she claims to be, and that the intended recipient of the message is indeed the one reading it. Digital certificates are issued by a Certificate Authority (CA), a third-party organization that both parties trust. The CA also generates digital signatures and public-private key pairs. Using a private key obtained from the CA, a recipient can decrypt a message, decode and verify the digital certificate, and know that the message is authentic. Similarly, if the recipient wants to send an encrypted message back to the sender, she can do so by encrypting it with the sender's public key. Through pre-existing relationships with trusted organizations such as financial institutions, the CA is able to guarantee the identity of individuals authenticating themselves with CA-issued digital certificates.[21] Individuals can also create their own digital certificates, but without external accreditation, such "self-signed" certificates carry less weight.

Human, technological and market failings are present in the dynamics of each

[18] Radio-frequency identification (RFID) smart cards have become popular recently for systems such as public transportation and tracking goods through a supply chain, and have recently been incorporated into newly issued passports in many Western countries. See, e.g., Anne Broache, RFID passports arrive for Americans, August 14, 2006, http://www.news.com/RFID-passports-arrive-for-Americans/2100-1028_3-6105534.html. However, many experts cite privacy concerns about the ability to more closely link people to their movements and activities, which have been aggravated by use of RFID chips in passports.

[19] National Institute of Standards and Technology, SmartCard FAQ, available at http://web.archive.org/web/20070711101540/http://smartcard.nist.gov/faq.html.

[20] See, e.g., Verisign: A History, http://www.verisign.com/static/036566.pdf (last visited 30 October 2007).

[21] Webopedia, Certification authority, http://www.webopedia.com/TERM/C/certification_authority.html (last visited 30 October 2007).

of these systems, especially when applied to tasks outside the four corners of their original purpose. Remembering one's username and password becomes increasingly difficult the more profiles one creates online. Smart cards are more secure, but they have to be carried around, and they are not fully interoperable worldwide. Furthermore, while they are physical objects, they contain software that is not unbreakable. Digital certificates are little understood by the greater community, and with some overhead to obtain, they are not widely utilized by typical Internet users. Biometric ID[22] raises substantial privacy concerns and (for better or worse) is not transferable. These methods of authentication are termed by security researchers "shibboleths," which come in three types: something you know (a password), something you have (a smart card or digital certificate), and something you are (a fingerprint or other biometric ID). More secure systems make use of more than one of these, but even then they are not foolproof, as the three types of shibboleths have also been facetiously described as "something you forget, something you lose, and something you cease to be."[23]

1.1.1 Definition: Digital ID Interoperability

Interoperability of Digital ID systems is an important issue in the ongoing discussion about how best to achieve strong and flexible authentication while successfully addressing privacy and security concerns. It is important to develop a clear definition of Digital ID interoperability, but no canonical definition has emerged. Such a definition must be broad enough to include the full range of possible identity solutions and their approaches to interoperability, from technical to procedural, whether implemented by private-sector cooperation or government action. In addition, as in our assessment of a DRM interoperability definition, it must not presume a preference for or against interoperability, and it must be flexible enough to include a range of levels of interoperability. Given the broad range of possible Digital ID systems and approaches to interoperability, this definition must be fairly broad.

For purposes of this work, we loosely conceive of Digital ID interoperabil-

[22] Biometric ID involves identifying a user by certain characteristics of her physiology or behavior, including iris or retinal scan, facial recognition, or voice identification. Each of these is increasingly used in the private sector, while fingerprints and DNA have well-known applications in identifying people in the law enforcement context.

[23] Wikipedia, Shibboleth (computer security), http://en.wikipedia.org/wiki/Shibboleth_%28computer_security%29 (as of 3 October 2007, 08:23 GMT).

ity as a constantly shifting interconnection among ID users, ID providers, and ID consumers that permits the transmission of Digital ID information between them via a secure, privacy-protected channel. It is also informative to think about interoperability from the perspective of perhaps overbroad stakeholder groups, including:

- Individuals (also referred to as users or subjects) – who want to be able to share aspects of their identity efficiently and securely regardless of the service or platform, with at least some level of ID portability;
- Relying parties (usually providers of services individuals want to use) – who want easy and secure access to accurate, timely, and relevant information about individuals from any source to maximize the value of their trust relationships and better serve their users, while limiting their own exposure to risks of a data breach;
- ID providers – who want effective and sustainable means to provide Digital ID services to any user and any relying party; and
- Society as a whole – which wants to balance convenient and secure authentication and accreditation with other social needs such as privacy.

1.1.2 Definition: Digital ID Innovation

Innovation in Digital ID likewise requires definition. For the purposes of this case, we define innovation as the process of developing and introducing new elements into products and services, noting that this occurs both within the digital identity "layer" and atop it. In a closed, proprietary sense, innovation can manifest as product updates and feature releases. In a more open sense, it can also include new developments by outsiders, including users, third party programmers, and even competitors of the original producer or service provider. Innovation can occur within the Digital ID space, in technology and in business models. As Digital ID has the potential to be an enabling technology, there is also the possibility of innovation happening on 'layers' above this space – in Web services, at the content layer, and in areas not yet conceived.[24]

[24] Jonathan Zittrain discusses the potential that a platform technology has to enable innovation at higher levels in The Future of the Internet – and How to Stop It (Yale University Press, forthcoming 2008). Eric von Hippel, among others, has also written about the

In contrast to the findings in our DRM case, we see there is a greater level of interoperability in Digital ID, and that there is a more widely shared sense that higher levels of interoperability might provide a viable solution to the identity challenge. For example, in May of 2005, Kim Cameron of Microsoft released "The Laws of Identity," a set of principles that developers of Digital ID solutions should take into account. The "Laws" were written as the result of a collaborative effort from individuals across industries and in academia, and have largely been adopted as strong guiding principles for a Digital ID infrastructure. While the developers of the Laws did not oppose non-interoperable systems, they concluded that an interoperable overarching infrastructure would benefit the Internet ecosystem by enabling individuals to use a wide variety of types of identities with different relying parties as appropriate to each transaction.

1.1.3 Models of Digital ID Systems

Digital ID solutions have thus far taken a variety of approaches. The models differ based on conflicting views about who ought to hold identifying data and who ought to control it. The models outlined below -- user-centric, federated and centralized -- each start from different basic philosophies – that users should control data, that data should be more or less widely distributed and trusted, and that data should be consolidated in a single repository, respectively. We recognize that these models are not rigidly defined and overlap in some areas. They may not exhaust the realm of possible approaches to the issue, but when taken together they cover the major efforts currently under development.

1.1.3.1 User-Centric Models

A user-centric model driven by privacy concerns aims to leave control with the user as to when and how their data is given to others. In a user-centric model, the user must initiate or approve any transfer of personal information before it takes place, either directly or through client or agent software with predefined rules for authorization. The degree to which a user is directly involved with each transaction varies; recurring e-commerce orders and automatic bill payments could be accomplished in a user-centric manner. The

importance of users modifying or adding new features to existing products. See generally Eric von Hippel, Democratizing Innovation (MIT Press 2005), available at http://web.mit.edu/evhippel/www/books/DI/DemocInn.pdf.

defining characteristic of a user-centric model is that it is philosophically and practically based on relatively active user consent each time identifying information is released, as opposed to company-authored privacy policies and one-sided terms of service. Consequently, the user and not the ID provider retains ownership of her data in a very real and practical sense.

To illustrate one example of a user-centric model, the following steps describe the sequence that CardSpace (see part 1.2.3 below) uses. This system begins with the individual obtaining various ‹cards,› which contain identifying information. This could be from, say, the individual's bank, verifying that they do indeed have money in the relevant account. The individual then virtually shows this card to a retailer, who learns 1) that the individual is indeed a breathing person with whom a bank has a relationship, and 2) that the person has money (and they may even learn how much). This differs from the current models of Digital ID because in a user-centric model, the retailer can get all the information it needs without asking for that which it does not require.

Table 1. The Transfer of Information in a User-Centric Model[25]

Steps in [the following] sample sequence, defined by Microsoft CardSpace and followed by compatible open-source projects such as Higgins and others, are as follows:

1. A certain user named Alberto uses the Firefox browser (or, rather, Firefox with an extension[26]) to go to the Best Buy[27] Web site. This site acts as the "Service Provider."

2. Best Buy's web page contains special HTML tags that are recognized by the Firefox extension as indicating that it is possible to sign-in using an I-Card, and that the site requires a certain set of information, or "claims" (e.g., name, email address, minimum age, etc.). The Firefox extension reads Best Buy's "policy" (i.e. what that Service Provider site requires in terms of claims and acceptable "token" types for secure packaging).

[25] Mary Rundle and Paul Trevithick, Interoperability in the New Digital Identity Infrastructure, January 2007, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=962701. This work is licensed under the Creative Commons Attribution-Share Alike 2.5 License.

[26] Some Identity Selectors require an extension to operate on some computer platforms and/or browsers.

[27] Best Buy does not actually support CardSpace at the moment.

3. The Firefox extension conveys the site's policy to Alberto's Identity selector and requests a token that conforms to this policy. Alberto's Identity selector then begins the "authentication" user experience. If this is the first time that Alberto has visited the Best Buy site, a page is displayed showing information about that Service Provider, including the site's level of security. Alberto next sees a dialog displaying his various I-Cards. Each I-Card represents a certain combination of data, or a claim. His collection of I-Cards might include, among others, one containing information from his driver's license and car insurance policy, another with his health-club membership information, and yet another with payment information and a shipping address. Unless Alberto's I-Cards were self-issued,[28] they each have an associated Identity Provider (e.g., a bank, government agency, etc.) that Alberto has designated to fill in the actual data (the "data values"). Alberto's Identity selector searches his collection of I-Cards to find those whose claims would match what is required by Best Buy. It then grays out (disables) the I-Cards that do not have the required claims and displays only those cards that fit the bill. Alberto selects the I-Card he wishes to use and clicks on it. He can also choose to push a button to preview the data elements associated with a card, and thereby review his name, age, current bank balance, etc. before releasing this information to a Service Provider like Best Buy.

4. When Alberto picks an I-Card and clicks on it, his Identity selector sends a request over the Internet to the I-Card's associated Identity Provider (in this case, the Bank of Canada), requesting it to provide the data values which Alberto has entrusted to it (e.g., "Albert" for first name, "over 18" for age, etc.).

5. The Bank of Canada as Identity Provider gathers the relevant data elements and wraps them in a cryptographically signed security token, which it then sends to Alberto's Identity selector.

6. Alberto's Identity selector sends the requested token to the Firefox extension.

[28] Most cards will be issued and signed by a third-party Identity Provider on the Internet, but the user can also make claims about himself. Such self-issued cards are less likely to be accepted by secure Web sites seeking third-party accreditation, however.

7. The Firefox extension sends the token to Best Buy. Finally, Best Buy unwraps the token and takes out the information that is needed for the transaction.

In many ways, this model mirrors the process that occurs in real space when an individual makes a traditional purchase at a store. The selection of the I-Card occurs just as people select a passport when traveling versus a library card when checking out a book. The issuing authority and the information contained match the needs of the transaction.

In its ideal form, a digital user-centric model would function better than real-life authentication in several ways. In our liquor store example from above, the individual shows a driver's license in order to verify that she is of legal age to buy alcohol. However, the driver's license contains all kinds of sensitive information the clerk does not need – name, address, height, unique identifying number, etc. In a more private environment, it should be possible to verify only the information required – that the individual holding the card is of legal drinking age.[29] For instance, in the case of Alberto, his card would only provide the necessary information, which includes his shipping address, minimal payment details and perhaps a way to contact him, in case his order is delayed.

A user-centric model must have at least a base amount of interoperability in order for an individual to use their digital ID for multiple services. The data format (such as XML, SAML, or OpenID protocols) and the authentication systems at the endpoints would, at the very least, have to support the proffered credentials. A greater level of interoperability would entail developing a consistent interface, such that the experience is seamless between sites. One could imagine a system whereby similarly situated retailers would request similar information in an identical way from their customers. In between common understanding of authentication credentials and completely identical ID systems, there are many ways user-centric Digital ID systems can interoperate with one another.

Interoperability between user-centric and non user-centric systems is also

[29] Perhaps we tolerate the excess information the clerk could obtain during the transaction because it is a brief, non-recorded encounter.

possible. For instance, an individual could have a credential allowing her to log into the site of her bank, which could then retrieve her account information from federated stockbrokers and banks, her employer, and tax authorities to present a complete financial picture without further user interaction. This would be possible even if her bank had a user-centric ID model but the tax authorities did not.

This model provides some additional benefits for the user. Though data can still be stored with a relying party once the data is given in a transaction, the user-centric model allows the individual to give minimal information. Thus, the relying party has much less to give away or lose (as in the case of a breach). The relying party can also benefit from such a model, as users are more likely to give better, more honest or more updated information when they are not being asked to for too much information, too often. Furthermore, the information provided by the user can be easily checked with the Identity Provider, causing greater accuracy and less potential for fraud.

A major drawback of the user-centric model is its complexity. There are significant technical challenges of creating a system that sufficiently satisfies all parties, such that they actually use it. With this come social challenges in educating business owners and users. Most web businesses are accustomed to asking users to provide identifying information – often more than strictly necessary – and users are used to providing it, and setting up a username and password for each site. This situation is familiar, if cumbersome. No understanding of technology or relationships involving third parties is necessary. In contrast, a user-centric Digital ID model requires both user and relying party to develop relationships with one or more trusted Identity Providers and possibly install and learn new software. Less tech-savvy individuals and relying parties may initially feel that the status quo is "good enough." This attitude could be a barrier to widespread adoption. Furthermore, because businesses that currently collect identifying data frequently profit by using it for marketing and/or selling it to direct marketers, they may be reluctant to give up control over their customers' data.

1.1.3.2 Federated Models

The federated model features network identity and user information stored across and recognized at various locations on the Internet. While the storage locations are linked such that information can be easily shared, there is no centralized control over the information. A federated model can also be user-centric if it allows the user to maintain control over which sites obtain her information and how much. The main characteristic of a federated model is a group of sites or systems, such as the UK Federation educational consortium,[30] that each trust the information about users provided by one another.

Once an "identifier" is agreed upon for a specific user, and that user has been authenticated by a federation member that she trusts, she will be able to navigate to any of the member service providers and be granted appropriate permissions based on her unique identifier that is shared among the multiple service providers. The process of establishing a shared identifier for a single user is often referred to as "federating" that user. The Liberty Alliance, described later, fosters federated digital identity models by providing protocols, and a way to test their interoperability.

Another example of a federated model is Shibboleth,[31] an open source project sponsored by Internet2 that allows a relying party to determine relatively seamlessly whether a user from another trusted system has the correct attributes or permissions to access a given resource. To illustrate how a federated system works, below is a slightly simplified description of how an individual would use a Shibboleth-based system. The particulars of other federated systems vary somewhat, but the principles will be similar.

Table 2. The Transfer of Information in a Federated Model

1. Betty, a researcher at Harvard University, needs to use an electronic database that she has learned is available to researchers at Oxford University. Betty has never been to Oxford and does not have a login ID at Oxford, but Harvard and Oxford are both part of a trusted Shibboleth federation.[32] She opens a web browser and pulls up the Oxford library web page, then clicks the link to the resource she needs, which is restricted to authorized users only.

[30] UK Federation, http://www.ukfederation.org.uk/ (last visited 10 October 2007). See also Joint Information Systems Committee, JISC introduction to federated access management animation, http://www.jisc.ac.uk/whatwedo/themes/access_management/federation/animation (last visited 10 October 2007).

[31] Shibboleth, http://shibboleth.internet2.edu/ (last visited 10 October 2007).

[32] Note that these two universities do not currently have such a relationship, but could establish one at any time.

2. Betty's browser is directed to a Where Are You From (WAYF) server, which attempts to ascertain her home site or Identity Provider. Betty might have to choose Harvard from a list of institutions including Oxford and other members of the UK Federation, or the WAYF server might be able to determine her home site automatically through software on Betty's computer or simply from the fact that her IP address is on the Harvard network.

3. The WAYF server, having learned that Harvard is Betty's home site, directs Betty's browser to a Harvard login page. This login might be implemented using the open-source Central Authentication Service[33] or any other system of authentication that can interface with Shibboleth. Betty, recognizing the familiar Harvard page, types in her Harvard user ID and password.

4. Harvard's server, after verifying Betty's user ID and password, sends Betty to Oxford's library server with an ID number (say ABC123) and a set of attributes (Harvard authorized user, staff, researcher, etc.). The ID number is specific to this transaction, and Harvard's server will verify it if Oxford's server requests it, but at no point does Oxford's server learn that it is Betty, specifically, who is requesting access to the database.

5. Oxford's server checks the list of attributes against the categories of users authorized to access the database. Although Oxford's server does not know the identity of user ABC123, it knows that she is a researcher and that researchers are allowed to access the database. Therefore, Oxford's server approves Betty and directs her browser to the database search page.

The level of interoperability within a federation is often fairly high, as they work best with seamless data transfer. The level of difficulty of a relying party joining a federation is more variable – for many, making it easy to have a large number of members is to their advantage. However, complex technical specifications or concerns about competitive advantage or security may preclude a federation – depending upon its rules and the technology choices made by its designers – from being open to new members. Furthermore, having

[33] Central Authentication Service, http://www.ja-sig.org/products/cas/ (last visited 10 October 2007).

many different types of institutions as part of the federation each with its own categories or policies regarding its own users may make it difficult for administrators to properly determine what categories of users should have access to each resource. Thus, scalability is a potential problem unless the federation is relatively homogeneous (as with British schools in the UK Federation).

Cooperation between federations is beginning to occur as federations identify partners beyond their initial offerings. In these cases, the offerings to the end user can improve substantially, but if the technology and rules the federations use are different, it can be difficult to implement these cross-federation initiatives. A base level of interoperability is needed in order to broaden the availability of the services provided by the federations.

However, some observers have expressed skepticism as to what extent and under what circumstances federations driven by for-profit corporations will benefit consumers. Just as companies that currently hold customer data often use it to profit directly (by selling it) or indirectly (by facilitating marketing and promotions), for-profit companies may seek to profit from federation, selling access to user databases to other online merchants. A wide variety of federated systems are possible, so the consequences for both corporations and consumers of federation in general are uncertain.

1.1.3.3 Centrally-Controlled Models

A centrally controlled model consists of one or more isolated repositories to which users give identity and user information. It can be one single (perhaps ubiquitous) source, or the ad-hoc repositories set up by most e-commerce sites in use today and other sites requiring registration. This centrally-controlled model is the dominant ID model in practice on the Internet today, yet it has few defenders as a system other than those who currently profit from it, as discussed above, through direct marketing and other related practices.

In a system with many ad-hoc repositories, when the user fills in a web form, the site owner takes that information and places it in a database. Sometimes the user has control over what data is kept in the repository, to whom it is released, and how long it is stored; more often, the site simply lists a privacy policy, outlining the ways in which they will use the data provided. For completeness, we will outline the undoubtedly familiar experience that our user from Table 1 would encounter with a centrally-controlled model.

Table 3. The Transfer of Information in a Centralized Model

Assume that Alberto, the user from Table 1, wishes to make a purchase from Best Buy but does not have CardSpace or another user-centric Digital ID program on his computer.

1. Alberto goes to Best Buy's Web site, chooses a product, and clicks the checkout button.

2. If Alberto has not bought from Best Buy before, he will be asked to register. He must type in his name, billing and shipping addresses, credit card information and security codes, and provide a username and password so he will not have to type all of this information in the next time he wants to buy from Best Buy.

3. After performing some verification of the credit card data provided, Best Buy processes the order and stores Alberto's information. Best Buy can make any use of this data permitted by its privacy policy,[34] and the next time he goes to Best Buy's Web site, Alberto can (if he remembers the username and password he provided) use some of the stored information, but will probably have to input the credit card information again to make fraud less likely.

A centralized model could also encompass a single source to which a user provides information, to which sites could send requests for specific identity data. This type of centralized control simplifies matters, but users are wary of entrusting all their data to a single source, especially one that is also holding everyone else's data. The single repository is also a single point of failure; if there is any damage to that repository, users may no longer be able to access their identity credentials, and if the database is breached, the hacker could get access to everyone's information. Providing a lot of data to Google Accounts (see Section 1.2.4 below), for instance, entails considerable trust in Google's security and reliability. Nonetheless, Google Accounts is somewhat user-centric in that users' information is only transferred after they specifically choose to log into a site.

[34] Best Buy's current privacy policy allows it to use users' personal information for advertising and marketing purposes, as well as sharing it with Best Buy "entities or subsidiaries," unless the user opts out. See Best Buy, Privacy Policy, http://www.bestbuy.com/olspage.jsp?id=cat12101&type=page&contentId=1043363533588 (last visited 10 October 2007).

The tendency of centralized control is to create information 'silos', in which data is stored in such a way that it is not sharable with others. If the information is simply walled off from those who would misuse it, this is a benefit. At the same time, information silos can limit the ability of a user to transact with whomever she chooses easily.

Interoperability among silos can occur, but integrating siloed data to create new services or facilitate existing ones is costly, cumbersome, and raises serious privacy and security concerns. This is so because, while federations are organized to interoperate securely, centralized repositories are usually implemented with security controls intentionally designed or incidentally constructed to create lock-in and make interoperability difficult. Service providers such as Facebook and LinkedIn have provided some degrees of interoperability with other data holders by making it possible for their members to enter log-in information for their email accounts and search their email address book for contacts with whom they are not yet connected on the service. To be sure, these efforts have the added benefit to the service provider of making it easier for users to help them grow the network, or to grow the number of connections within the existing network. (Not incidentally, this method of interoperability does not require the other data providers' consent, which otherwise would have to be negotiated and paid for.) Similarly, financial services like Quicken and Yodlee allow a user to input all the various passwords and other security information for their banks' Web sites and then view a consolidated financial picture in one place. However, these ad-hoc methods of linking centralized data repositories have obvious privacy and security drawbacks. But for whatever internal security procedures are in place at these companies and despite what the terms of service may say, rogue employees at Facebook or LinkedIn could peruse the e-mail of users who avail themselves of the integration service, and Yodlee and Quicken could pry into their customers' financial affairs or even steal their money with remarkable ease. Taking part in these programs necessitates an enormous amount of trust that, in view of high-profile data leaks in every sector of the economy, may not always be justified. Even if Yodlee and Quicken are completely trustworthy, the hacker who finds a way to break into their systems or the thief who makes off with their backup tapes will not be. And it goes almost without saying that, once a centralized ID provider has a consumer's data, it may make uses of it that the consumer might not have authorized if asked specifically, but are permitted by the ID provider's privacy policy.

In the case of government organizations, which often use a centrally-controlled model to hold identity information, efforts towards interoperability are underway. In the European Union, directives that aim to enable information to cross borders, such that a citizen of one EU state might have greater capabilities to do things such as access her bank, obtain a mortgage, or claim unemployment benefits while traveling in another EU state, have been adopted.[35]

In the United States, Homeland Security Presidential Directive (HSPD) 12, released in August 2004, mandates interoperability between databases of different government organizations in an effort to increase knowledge sharing and national security.[36] As the United States government is both a producer and a consumer of information, it has a vested interest in making identity information at least internally accessible. Interoperability could have the positive effect of enabling greater ease of services – or could engender privacy concerns that are aggravated by information sharing.

1.2 Experiences with Digital ID Interoperability to Date

Interoperability is possible between sites and between ID systems. In the past, the fact that computing did not begin with communication between machines was a major hurdle to interoperability in this context. When Unix was written in the late 1960s, each model of computer required specialized translators to share data with other models.[37] Today, standardized tools and methods enable the formation of large networks comprised of thousands of different brands and models of computers with relative ease. Standards organizations such as IEEE and OASIS keep track of various protocols, and by making standards known and available, they enable interoperability between new and old products.

[35] A Roadmap for a pan-European eIDM Framework by 2010, http://europa.eu.int/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf (last visited 30 October 2007).

[36] Homeland Security Presidential Directive 12, August 27, 2004, http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.

[37] David Upton, Bradley Staats, and Trent Staats, Information Technology Tutorial (Harvard Business School Press, 2006).

Most attempts to solve the problems associated with Digital ID involve creating some kind of system that would serve as a layer of communication between service providers. The processes to create such a layer involve either some kind of standards process – open or proprietary - or the *de facto* (emergent) adoption of common technologies. The following approaches towards an emerging Digital ID infrastructure consist of methods that illustrate the variety of ways in which stakeholders view the problem and its possible solutions. We do not attempt here to exhaustively survey the many initiatives currently underway, but only to analyze a few projects that collectively represent the various trends at work in the market.

If identity is to be embedded in the Internet, identity protocols must be interoperable. Communications take place across well-accepted layers of the Open Systems Interconnection (OSI) model (see Appendix). The addition of an identity infrastructure could sensibly establish another 'layer' in the OSI framework, enhancing interoperability across all users of identity on the Internet. Even more modest, less interoperable efforts, though, still have much to offer in user privacy and convenience and in service integration.

1.2.1 Example #1: Liberty Alliance

The Liberty Alliance was formed in 2001 by approximately 30 organizations to establish open standards, guidelines and best practices for federated identity management. It has 150 members today, including AOL, Fidelity, Sun Microsystems, Novell, Intel, Oracle and HP. The Liberty Alliance has developed protocols, some of which are now at OASIS, and helps developers to test their implementations of Liberty protocols against others, to ensure that they interoperate in the way that was intended. Thus, it ensures that consumers and users of Internet-based services and e-commerce applications that employ such implementations can authenticate and sign on to a network or domain once from any device, and then visit or take part in services from multiple Web sites. This federated approach does not require the user to reauthenticate and can support privacy controls established by the user. The main goal of Liberty is to increase the ability of parties to share in greater trust online, ideally with protocols built in a collaborative way that provide low barriers to entry for new parties.

1.2.2 Example #2: Higgins

The Higgins Trust Framework (formerly Eclipse Trust Framework) is an open source software effort, begun by members of the SocialPhysics project.[38] Higgins is a software framework that relies on middleware service adapters that connect to external systems using that system's native protocols or APIs. Higgins' goal is to give users more control of their online identity, profile and relationship information. Applications written with the Higgins API can integrate the identity, profile, and relationship information across heterogeneous systems. The intention of Higgins is to become "glue," simply connecting systems together and providing a platform on which to easily create new connections. This goal caught our attention because it is very different from the approaches taken by other Digital ID systems, which were at least initially intended to compete with or replace one another, rather than bringing competing systems together.

Within the Higgins framework, developers can exchange plug-ins and APIs for various preexisting identity systems as they become available. According to Higgins' project goals, Higgins "introduces a new 'context' abstraction and allows developers to create adapters to legacy systems." [39] In other words, instead of introducing another new identity system, Higgins connects identities across system boundaries. Higgins also provides an end user with a Digital ID experience based on the "i-card" metaphor, through which it interoperates with a growing number of identity protocols such as Microsoft CardSpace, OpenID. Work, supported by Google, has begun on adding SAML 2.0 support as well.[40]

According to IBM, which has contributed code to the Higgins project:

> [The Higgins framework] breaks up a person's identity into pieces – or 'services' – and lets computer users dictate who can access what parts of their identity information, within applicable privacy guidelines and laws. Organizations using 'smart' applications, built with Higgins open source tools, can share specific identity information, such as their telephone number or buying preferences, according to rules set by the individual, or by an authorized third-party service provider acting on their behalf. Like Web services, companies will be able to build support

[38] By way of disclosure, the Berkman Center for Internet & Society has been closely involved in the development of the SocialPhysics project, especially through the work of Fellow John Clippinger.

[39] Higgins Trust Framework Project Goals, http://www.eclipse.org/higgins/goals.php, (last visited 30 October 2007).

[40] E-mail from Paul Trevithick, October 25, 2007.

> for Higgins into their applications, websites and services, and its open approach will support any technology platform and identity management system.[41]

IBM, Novell, Parity Communications, Oracle, Microsoft, the Liberty Alliance and others have been very supportive of the Higgins effort. IBM and Novell have each allocated significant engineering resources to the project. However, it remains to see, when all is said and done, how many of the players will adhere to an open standard.[42]

1.2.3 Example #3: CardSpace

Microsoft created CardSpace in an effort to implement its own system of user-controlled digital identity. This was not Microsoft's first experience in the identity space. As an initiative, CardSpace stood out from Passport and Hailstorm, Microsoft's two earlier attempts to create identity management systems. Passport and Hailstorm were closed, highly centralized systems, and many users did not feel comfortable providing a large corporation such as Microsoft with all of their personal details.[43]

CardSpace works in an identity infrastructure under tenets similar to those employed by Higgins; specifically, that identity works best (and safest) when it can be parsed into usable "chunks" and shared on an as-needed basis. CardSpace works on a user-centric model as described above. Thanks to support from Microsoft, CardSpace has been or will be made interoperable with the Higgins framework, Liberty Alliance protocols, and OpenID, among others.

CardSpace currently works with other Microsoft applications such as Windows operating systems and Internet Explorer. Other implementations, such as the open-source Bandit project sponsored by Novell, also work with CardSpace services. The protocols behind CardSpace are published and available royalty-free, with the hope that developers will use the protocols to extend its capabilities to other platforms and applications. If this happens, CardSpace could provide an interoperable Digital ID system.

[41] IBM Corporation, Open Source Initiative to Give People More Control Over Their Personal Online Information, February 27, 2006, http://new.marketwire.com/2.0/rel.jsp?id=682795&sourceType=1.

[42] E-mail from John Henry Clippinger, May 29, 2007.

[43] Dick Hardt, Why Passport did not become Ubiquitous, December 7, 2004, http://blame.ca/dick/?p=35.

1.2.4 Example #4: Google Accounts Authentication

In July 2006, Google released its centralized account authentication service. Google provided code that helped developers creating web applications to utilize Google's account access features in order to protect their web applications from un-authenticated users. In other words, access to a developer's own web – or installed – application could be granted once the user supplied her Google username and password.[44] When Google first released the API for these, it fell under much scrutiny. For example, Dick Hardt, founder of Sxip and a proponent of user-centric identity models, stated that Google Accounts Authentication (GAA) was moving identity management "two steps forward, one step back," because of the centralization of users' identities deeper into what Hardt called the "Google identity silo."[45] An alternative approach might be to allow a user to access a site or application built with the GAA API using a non-Google credential, although the consequences of doing so would be uncertain.

In this model, the developer can choose to specify whether authentication requires secure tokens or non-secure tokens. The use of secure tokens requires that the web application be registered with Google and file a certificate; if registered, the web application can secure all requests referencing an authentication token with a digital signature. This distinction between the use of secure versus non-secure tokens will certainly influence the type of web applications that utilize GAA API. For example, GAA may work well with a non-secure token if the user wants to log into a news site to read an article, but that same insecure login would appear unattractive to a user hoping to make a purchase online; exchange of monetary information clearly necessitates the highest levels of security. User education will be important to prevent phishers and poorly configured Web sites from inappropriate use of the less secure GAA API.

- When the web application needs to access the user's Google service data, it directs the user to the Google Accounts URL.

[44] Google Inc., Account Authentication, http://code.google.com/apis/accounts/Authentication.html (last visited 30 October 2007).

[45] Dick Hardt, Google Account Authentication: Two Steps Forward, One Step Back, http://identity20.com/?p=62, June 28, 2006.

- Google Accounts responds with an «Access Consent» page. This page prompts the user to log into their Google Account and grant/deny access to the service.

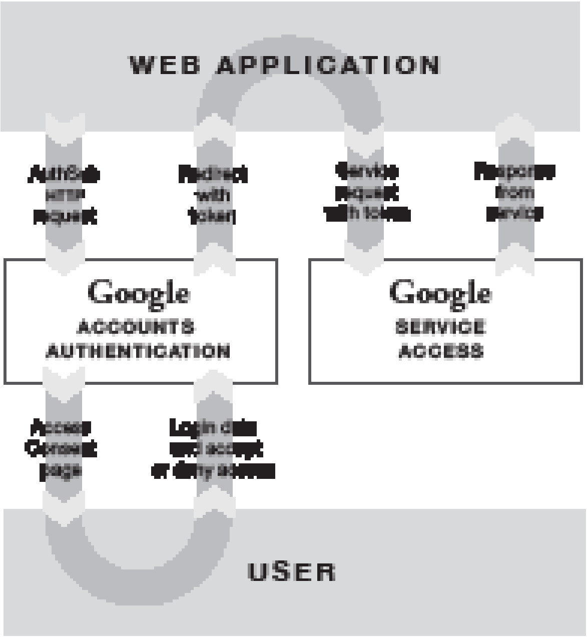
- The user logs into their Google account and decides whether to grant or deny access to the web application. If the user denies access, they are directed to a Google page rather than back to the web application.

- If the user successfully logs in and grants access, Google Accounts redirects the user back to the web application URL. The redirect contains an authentication token good for one use; it can be exchanged for a long-lived token.

- The web application contacts the Google service to confirm the authentication token.

- If the Google service recognizes the token, it will supply the requested data.

The Authentication Proxy diagram shown below illustrates interactions between the three entities involved: web application, Google servers, and the user.



Google's APIs make it easy for non-Google applications to consume Google services, but they are tied to the user's Google credential. While increasing the value of that Google credential, this system also creates a bigger barrier to competing services and increases the users' reliance on the Google credentials. As with CardSpace, the arrangement of open protocols could provide some degree of de-facto interoperability between different identity management solutions. However, given the core importance of trusted Google servers to the GAA framework, it is not clear what GAA would be without linkage to Google credentials. Therefore, there is reason to question the long-term sustainability of a Digital ID infrastructure based on GAA as it currently exists.

1.2.5 Example #5: Shibboleth

As described above in Table 2, Shibboleth is an open-source, federated Digital ID system designed initially to allow universities and other academic institutions to share resources. Although it was initially designed by Internet2, others have contributed to it. In particular, Microsoft has sponsored work to integrate Shibboleth with CardSpace. Like Higgins, Shibboleth is agnostic about what technology is used by the servers at each endpoint, and it was designed in part to enable diverse existing login schemes to interoperate with one another. In that sense, its strength and its weakness is that it is an incomplete solution to interoperable Digital ID. On the one hand, each system connected to a Shibboleth federation can have a different system for users to authenticate, whether it be CardSpace, CAS, or something else, but on the other hand, each system must have another software solution on top of Shibboleth for it to be useful (otherwise users have no way to access Shibboleth). Some administrators might find it easier if they only have to install and administer a single authentication system.

1.2.6 Other examples

Open, industry and user-driven efforts towards interoperability and user-control in digital identity have emerged in recent years. Additional examples include open source projects like OpenID and proprietary efforts like Microsoft Live ID. The goals differ from one to the next, but they each aim to pull standards efforts, technologies, and incentives together to create an emergent identity infrastructure that developers can build upon and companies and consumers will use.

These examples show the myriad ways in which efforts towards better Digital ID have so far manifested. Competition between companies has provided much of the motivation for these initiatives, as they either attempt to provide ID solutions or require good ID solutions for their value-added services. In the next section, we will discuss a range of incentives in more depth.

1.3 Forces at Play: Some Drivers and Inhibitors

As with DRM, interoperable Digital ID is a complex system. The technology required to build, maintain, and secure the system gives rise to a constant cat-and-mouse game between developers and data holders on the one hand and those who seek to steal personal data on the other. In addition, a host of market forces provide incentives and disincentives for competition and cooperation. Societal opinions, especially surrounding privacy and surveillance concerns, press companies and governments to consider legal regimes that protect individuals even as individuals currently sign away their privacy through user agreements and privacy policies on a regular basis. Yet stronger government action could actually slow the process of developing Digital ID interoperability by freezing technological development or imposing significant burdens on one or more stakeholders. This section will attempt to lay out some of the drivers and inhibitors of interoperability in Digital ID.

1.3.1 Technology

As shown by the processes outlined in the previous section, the technology underlying an ID infrastructure is complex, but there are numerous examples of at least some level of technical interoperability working. Consider, for example, efforts to centralize government-issued identification. In the United States, technical interoperability was achieved with government employee identification,[46] and in Portugal, a recent initiative centralized five different government ID cards into one system, making all the information accessible to the agencies that need it and to the citizens.[47] However, also in the United States, there has been strenuous resistance to just the sort of single, national

[46] See, e.g., Daniel Pulliam, Federal employees begin receiving new ID cards, October 26, 2007, http://www.govexec.com/story_page.cfm?articleid=35363.

[47] See Andre Vasconcelos, The Portuguese Interoperability Framework applied to the Portuguese Citizen Card Project, presented at the OECD Workshop on Digital Identity Management (IDM), May 9, 2007, http://www.oecd.org/dataoecd/36/9/38573902.pdf.

ID that was achieved in Portugal.[48]

Many protocols for messaging and data exchange have developed through standards processes or subsequently been released openly. For example, Security Assertion Markup Language 2.0 (SAML 2.0) was developed under OASIS and ratified in 2005 as its standard, and includes input from the open source project Shibboleth and from the Liberty Alliance.[49] Most of the underlying protocols used by CardSpace (WS-Trust, WS-MetadataExchange, etc.) have also been submitted to OASIS. Furthermore, in May 2007, Microsoft announced an extension to its Open Specification Promise to cover most of the protocols and specifications behind CardSpace 1.0.[50] It thus committed to providing access to its CardSpace-related identity solutions and protocols on an open, royalty-free basis.

The Higgins project aims to create software to allow technical interoperability between diverse systems and bridging across multiple protocols. It has already achieved substantial interoperability among some of the major Digital ID systems, and continues to make progress on breaking down technical barriers.

The area of technical security requires mention, as the arms race between security developers and malicious hackers could present a barrier to the development of a standard on which to base a highly interoperable Digital ID system. With identity fraud and other unsavory business models now providing financial incentives for thieves of identifying information, this issue is only growing. A lengthy standards process that attempts to build in security as part of its protocols could easily fall behind in the arms race before it is implemented. It is heartening, however, that SSL and its successor TLS, which has developed through a public Request For Comments (RFC) process, are still sufficiently secure to enable widespread e-commerce despite many years of hackers undoubtedly trying to break them. Though creating such standard protocols is difficult, it can be achieved in this context, and once agreed upon,

[48] See Electronic Privacy Information Center, National ID and REAL ID Act, http://www.epic.org/privacy/id_cards/ (last visited 10 October 2007).

[49] Liberty Alliance, Liberty Tutorial, http://www.projectliberty.org/liberty/content/download/423/2832/file/tutorialv2.pdf (last visited 30 October 2007).

[50] Microsoft Corporation, Microsoft Focuses on Interoperability for the Identity Metasystem, May 23, 2007, http://www.microsoft.com/presspass/press/2007/may07/05-23-MetasystemPR.mspx.

standards can be updated in an evolutionary fashion. We conclude that technology problems, while no doubt challenging, do not amount to a significant independent barrier to interoperability.

1.3.2 Multiple Market Forces Behind Adoption

The Digital ID infrastructure is a network effects business, meaning that widespread uptake is required for the whole system to succeed – the more users participate, the greater the incentives to support them through a broad variety of market offerings. For businesses that provide ID solutions, the desire for interoperability with other systems may change depending on whether they believe they can create a sufficiently large network alone, versus depending on others to aggregate a large enough network to be useful to consumers. In the commercial Digital ID space, so far the market has rejected the idea of a single dominant player.[51] Therefore it appears to be strongly in the ID business' interest to grow the market as a whole, rather than fighting for a large share of a small market. This may indicate that the ID business' incentives are aligned with interoperability. However, those working in e-commerce, even within the same company as those creating Digital ID solutions, may have a different view. Network effects could induce e-commerce professionals and other stakeholders to support an interoperable solution as well, but only once such a solution became a standard or gained significant user adoption. Service providers want to make it as easy as possible for customers to use their services, but will not make the potentially substantial investment in changing their authentication infrastructures to interoperate with Digital ID systems that only a handful of customers will use. An analogy can be made to web design – once Microsoft's Internet Explorer (IE) web browser became dominant, web designers only wrote web pages with IE in mind and tested them

[51] For example, Microsoft's Passport was intended to be the full provider of identity management online, in part because users were wary of storing personal information in a central Microsoft database. ZDNet UK, Passport failure shows the folly of Microsoft's ways, January 4, 2005, http://opinion.zdnet.co.uk/leader/0,1000002208,39183062,00.htm. Around 2001, users started to bristle at the amount of information Microsoft appeared to be collecting from them, as well as the emerging security threats introduced by the integration of Passport and the Windows operating system. Users were also worried about the lack of transparency. Dick Hardt, Why Passport did not become Ubiquitous, December 7, 2004, http://blame.ca/dick/?p=35. Companies were not able to adopt the technology easily either – Microsoft's licensing, at $10,000, was out of reach for many small businesses. It is interesting, given this history, that Google Accounts and Microsoft Live ID each appear to be once again attempting a centralized Digital ID solution, albeit without the high price tag.

to make sure they worked in IE. When Firefox (as well as Safari, Opera, and others) gained non-negligible market share, Web site owners had to go back and make their sites Firefox-friendly or risk losing customers who use Firefox primarily or exclusively. Until such a tipping point is reached, however, many service providers will resist interoperability.

Among businesses engaged in e-commerce in particular, incentives towards interoperability are weaker than among their ID business counterparts. This is especially true for companies engaged in the sale of products that can be termed e-commerce commodities – airline tickets, books, electronics, and the like. In this space, all that may be keeping a buyer going to one site over another may be the reality that the first site already has their log-in information, credit card numbers and preferences.[52] Even though this lock-in may be fleeting, any part of the transaction process that can keep a customer creates incentives against interoperability. For businesses where information on previous transactions and habits can significantly enhance the customer experience, the ability to access an account's history can establish more lasting lock-in.

In addition, for an e-commerce business, ID is only one factor of their business model. Their greatest concern is that it work, preferably as unobtrusively as possible. Successful e-commerce merchants already have a customer base in their existing systems, and so have low incentives to change absent consumer demand. This explains in part why the process towards Digital ID interoperability has seen fewer champions from the e-commerce space than from those interested in providing ID solutions.

Market maturity also plays a strong role as a lever on interoperability of the Digital ID space. Interoperability may flounder if implemented too early in an emerging market, as the optimum technology and legal and social regimes are not yet obvious and stable. Any official initiative towards interoperability could be unsuccessful, as firms may innovate at a rate faster than the standards process.

There are some examples in which organizations seem to benefit from providing Digital ID interoperability. One area includes social networking sites, which have begun providing interoperability on an ad-hoc basis. The ex-

[52] Interview with Isabel Hilborn, June 12, 2007.

amples of Facebook, LinkedIn, Quicken, and Yodlee make it possible for the user to import information from another service. However, this capability is rarely bi-directional, nor does it increase interoperability across the system in a widely meaningful way.

Some companies are based around the idea that strictly 'transaction' economic interests are too narrow. In the Web 2.0 era in which user communities, user experience and flexibility in the way individuals interact with the Internet are necessary, such companies are looking to extend their interactions with the user beyond the transaction. They are looking to compete on the layers superimposed on top of the ID layer, rather than within the ID layer as we saw above. For these, incentives may be more closely aligned with interoperability of Digital ID because they are looking to compete at the next level – services – instead of at the identity layer. While these enterprises may seek to retain customers by making interoperability with competing services difficult, they support Digital ID interoperability because a substantial user base is necessary to create the market for which they compete.

1.3.3 The Role of Law

The law might play a role in shaping or maintaining interoperability of Digital ID systems. While intellectual property protection (e.g. protection of protocols) and antitrust issues (e.g. standard-setting bodies, cartels, leveraging of market share) may play a role similar to that in the area of DRM (see DRM case study for further details), two issues seem of particular importance in the area of Digital ID systems.

First, if any interoperable Digital ID system is to emerge, all parties involved will benefit from understanding how liability will be allocated in the event of chargeback or fraud perpetrated through the system. In particular, what happens if a trusted member of a network is compromised? Because more and more transactions are occurring online, there are more criminal or fraudulent transactions online as well. In an interoperable Digital ID ecosystem it may be unclear which part of the system would assume liability for the credentials that are issued, and for the security of the transaction system. The structure of Liberty Alliance, for example, is based upon large companies forming "Circles of Trust," which are tasked with part of the system or data, but so far there is no clearly delineated method for dividing responsibility. Whether there is need for ID-specific law to regulate liability or whether a careful design of contracts can – and actually will – manage to sufficiently allocate liability exposure[53] is an open question. Therefore, *legal uncertainty* with regard to liability exposure in a multi-player Digital ID ecosystem may already have exerted and continue to exert a chilling effect on the establishment of Digital ID interoperability.

Second, *legal diversity* may act as an inhibiting force to interoperable ID systems, especially in the governmental context. As there are incentives to provide interoperability between government databases – e.g., the ability to more effectively share information relevant to national security – several harmonization efforts have been executed. For example, when introducing a new "Buergerkarte" (identity card), the Austrian government worked closely with other European countries to integrate their respective ID capabilities.[54] However, *subsidiarity* concerns, pushing for smaller, simpler processes and organizations, as well as cultural differences between countries or regions[55] may work against a full harmonization of legal requirements.

From a user standpoint, an identity infrastructure can provide great convenience and raise privacy concerns. As individuals move with greater frequency from place to place, disparate agencies can share information to enable services to follow more seamlessly.[56] However, if the government can find you to update your driver's license, it can also find you to monitor your communications. Greater government capability in this regard creates at least some erosion of individual privacy. It is unclear, however, where government use of Digital ID is likely to fall on the spectrum from identifying citizens so they can vote online to an intrusive policeman tracking every online act.

[53] See Manel Medina et al., Fidelity: Federated Identity Management Security based on Liberty Alliance on European ambit, http://www.celtic-fidelity.org/fidelity/Documentation.jsp?download=48 (last visited 30 October 2007): "All of them [i.e. circles of trust of the Liberty Alliance Project] should sign commercial, business and service agreements, through which they regulate their rights and duties to handle users attributes to provide tailored services to the users in the most transparent and user friendly way."

[54] See Austrian Citizen Card, http://www.buergerkarte.at/index_en.html (last visited 26 October 2007).

[55] Cf. Modinis-IDM, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi (last visited 26 October 2007).

[56] For example, in Massachusetts, the U.S. Postal Service will periodically share address change information with the Registry of Motor Vehicles, enabling them to send out address change stickers for driver's licenses. To be sure, this also enables enforcement of such things as resident parking.

2 ASSESSING DIGITAL ID INTEROPERABILITY

2.1 Potential Benefits

Interoperability of Digital ID would bring both benefits and drawbacks for consumers. Many benefits and drawbacks will not become fully clear until the technology becomes more mature and innovative applications start to emerge, but some plausible predictions can be made. Among the projected benefits of interoperability in this context are ease-of-use, privacy, anonymity and low price. An interoperable Digital ID system could also grow the Internet economy as a whole by enabling new areas of Internet-based transactions. Most of these characteristics are made possible by interoperable single-sign-on systems. Demand for low price is probably best satisfied by competition among ID providers, and interoperability allows them to move between competing providers without prohibitive switching costs.

Digital ID interoperability might help digital identification map more closely to the way identification happens in the real world, as identification in real life is approaching interoperability in many cases. Consider, for example, that passports are becoming more ubiquitous, and are accepted identification for many services – ranging from identity verification when boarding an airplane to verification of employment eligibility. If Digital ID were interoperable in a similar way, user confusion might be reduced. Moreover, as mentioned above, an interoperable Digital ID system would enable the user to easily choose the relevant set of credentials or information to transmit – so a user could have a “passport” that could be used for many applications, but would not actually have to convey all the information contained on her passport in order to check out a library book.

In addition, an emerging Digital ID infrastructure could include greater privacy control, reducing the social and financial risk that users incur when online. Overall, interoperable ID systems make it easier for users to engage in online transactions because they do not have to create new credentials for each site or each of several incompatible ID schemes. Interoperability gives users flexibility and choice by reducing the transactions costs associated with authentication and/or accreditation.

The potential growth of e-commerce with Digital ID interoperability is significant, and the emergence of a layer of companies that provide Digital ID services is another potential area of market growth. The implementation of such a system would provide a platform for the development of value-added services on top of it.

With seamless authentication and payment could come a layer of Web services-enabled systems that require secure transfer of trusted information. Consider a service in which a call from a GPS-enabled mobile phone to a taxi company could automatically provide location and payment information.[57] Anonymous but verifiable authentication could also transform the local, trust-based commerce models of Craigslist and classified ads more generally.

Interoperability of ID infrastructures is likely to increase innovation and competition between online companies at the ID layer and at the layers above, as customers could easily switch without renewed identification. As competition then increases incentives to innovate in similar fields, we consider it to be a key potential benefit of Digital ID interoperability.

2.2 Potential Drawbacks

Drawbacks can be found both in the process towards interoperability in Digital ID and in the actual implementation of such a system. For one, though significant standard-setting processes have occurred, it remains to be seen how deeply committed the large players are to these standards.[58] Since this is a market in which user uptake must be widespread, standard-setting efforts

[57] Interview with Eric Tiffany, June 13, 2007.

[58] E-mail from John Henry Clippinger, May 29, 2007.

that do not engender wide support could hold back the potential for market growth. Confusion over competing or incompletely compatible standards could also result in companies sitting on the fence, waiting for the space to settle out before acting.

Interoperability in Digital ID could also endanger businesses that depend on consumer lock-in for their customer base – which presents a drawback from the perspective of such businesses and their shareholders.[59] However, given the low barriers to entry in terms of authentication (simply setting up a database of usernames and passwords), interoperability could also provide an opportunity for such companies to poach competitors' customers.

Security presents an additional potential drawback, as the security of an ID system could be endangered by the mere fact of more parties having access to a certain ID, which increases the potential of misuse. Depending on the protocols and implementation, it might be more difficult for a breach or leak to be repaired once one occurs. Certainly, if any level of trust is involved, a breach can have more widespread consequences. A hacker able to successfully impersonate any trusted server would have carte blanche for identity theft or disrupting the entire trust network.

Though giving complete data to fewer parties enhances privacy, with interoperability, a single party might end up in possession of much more information about a certain user than in case of non-interoperable identity-silos. Once a user authenticates to a site, it might be able to request a wide variety of other information from federated sites. This could also raise the potential for misuse.

Finally, we can envision a scenario in which too much ease of use could prompt "identity" to be used for things where the consumer does not really want it, forcing authentication into places and activities where one could formerly be anonymous. Some of the most valuable applications of the Web are possible because the medium is anonymous, or at least relatively so. It would be a great loss if interoperable Digital ID became ubiquitous in ways that erode the potential for anonymous (or at least quasi-anonymous) communication on the Web. In addition, the trend of more sophisticated phishing is worrisome in this regard, as consumers might transmit considerable information to spoofed Web sites by accident.

[59] Interview with Isabel Hilborn, June 12, 2007.

3 APPROACHES TOWARDS DIGITAL ID INTEROPERABILITY

Several approaches towards Digital ID interoperability are on the table. In general, Digital ID interoperability is in a later stage of development than DRM interoperability and is more complex than interoperability in the mashups context. That said, full interoperability is a long way from being achieved in the Digital ID space. We will discuss several main approaches in the paragraphs below.

Interoperability in the Digital ID environment might be accomplished by a range of means, several of which are in progress. Non-regulatory, non-government approaches include:

- Ad-hoc or de-facto interoperability. As mentioned above, services such as Facebook, LinkedIn, Yodlee, and Quicken have provided ad-hoc and as-needed interoperability to users, in ways that increase the value of their services (if potentially opening themselves to greater liability for holding even more user data, unless they successfully disclaim it in their terms of service).

- Open source, carrier-neutral projects. In recent months, Higgins has seen buy-in from most major players, and the mission of the project aligns with the goals of major stakeholders. This 'glue', if development and buy-in continue, could provide the type of generative interoperability that would allow a range of Digital ID solutions and business models at the ID layer, and could encourage innovation at upper layers.

- Standardization and technical collaboration. As mentioned previously, technical interoperability is not sufficient for an interoperable Digital ID infrastructure, but it is a necessary condition. Without technical collaboration, only the ad-hoc interoperability described above is likely to occur. But if major stakeholders do not work together to integrate and market a system as interoperable, user adoption will continue to be limited. Standards can lead to interoperability, but only if relevant parties adopt and implement them. In addition to the standards processes mentioned above, the ISO and W3C are forming working groups on privacy and ID systems, but so far no results are presented.[60]

- Licensing and unilateral design. As seen by experiences with Passport and Hailstorm, a unilateral approach is a possible route to a kind of unanimity of experience for users, but is highly unlikely to lead to interoperability in such a complex environment.

Regulatory and government-initiated approaches are also being tested in some areas. As seen in previous sections, governments are working to make their own systems interoperable, and they are pressing others to be interoperable as well. They can encourage this in several ways:

- Broad initiative. The EU's Roadmap for a pan-European eIDM framework by 2010[61] is one major example of governments encouraging interoperability by sweeping plans across the board.

- Subsidies. The PRIME Project (Privacy and Identity Management for Europe), which is funded by the European Union, is strongly focused on encouraging a user-centric experience.[62] The GUIDE Project, in the eGovernment area, is also funded by the EU and conducts research and

[60] See Marit Hansen and Martin Meints, Digitale Identitäten – Überblick und aktuelle Trends, September 2006, http://www.fidis.net/fileadmin/fidis/publications/2006/DuD09_2006_543.pdf (in German only).

[61] Available at http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf

[62] See Marit Hansen and Henry Krasemann, eds, Privacy and Identity Management for Europe – PRIME White Paper, Jul. 18, 2005, https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V1.pdf.

technological development that seeks to enable EU countries to provide eGovernment services seamlessly.[63]

- Cooperation between governments. While country-based solutions are useful for programs administered at the national level, the Internet enables many projects that cross national boundaries. Where governments cooperate in offline endeavors, it makes sense for them to connect in the Digital ID space as well. As especially EU governments work to implement an ambitious plan for interoperability by 2010, they have encouraged focus on the issues associated with achieving this goal – they have encouraged dialogue between stakeholders, and provide a willing customer to ID solutions businesses.[64]

- Mandating standards. As with the Homeland Security Presidential Directive mentioned previously, governments have also approached achieving technical interoperability by mandating standard data formats, which is important in data exchange between countries, or between agencies within a country. However, such standardization could have serious consequences in the event of a data breach like those we have seen in the commercial realm.

- Public procurement. In Finland, for example, the tax board implemented Liberty Alliance procedures to test the interoperability of several e-governance solutions they were implementing.[65] The result was a high degree of effectiveness in their implementation, which now allows for strong authentication and ease of a number of new services.[66]

- Encouraging dialogue. Groups such as the Organisation for Economic Cooperation and Development (OECD) have encouraged Digital ID interoperability by fostering research on solutions and dialogue between stakeholders.

[63] Creating a European Identity Management Architecture for eGovernment, http://istrg.som.surrey.ac.uk/projects/guide/ (last visited 30 October 2007).

[64] For one such example, see Modinis IDM, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome (last visited 30 October 2007).

[65] The Finnish National Board of Taxes Makes a Business Case for E-Authentication, http://www.projectliberty.org/liberty/content/download/417/2814/file/Finland_casestudyFINAL.pdf (last visited 30 October 2007).

[66] Id.

So far, we find no evidence that regulatory processes are currently underway to establish commercial Digital ID interoperability. There is no single dominant player in this environment, which has precluded most inquiries into competition or anti-trust issues, a typical entry point for government involvement in commercial affairs. (In contrast, France's DRM interoperability clause was inspired at least in part by Apple's large market share, for which there is no analogue in the Digital ID story to date.) Furthermore, the lack of broad consumer demand had allowed the spotlight to remain on more visible issues like DRM and Internet neutrality.

4 SUMMARY

We conclude from this case study of Digital ID systems being built for the Internet that there is no single, clear path to the sort of interoperability that will lead to further innovation on the horizon. That is not to say that there is not interoperability between some leading systems; nor is it to say that interoperability would not be a good thing in terms of leading to innovation. The point is that there is no "silver bullet" approach to accomplishing ID interoperability in this context.

An interoperable Digital ID system for the Internet could lead to more secure, more private, and more efficient identity management. Significant market and legal forces combine to make implementation of any single, interoperable system a complex process; uptake is far from assured.

The multiple approaches to interoperability that are in progress in this field cover a broad range. On one end of the spectrum, informal groups of firms are collaborating through ad hoc networks; on another end of the spectrum, an interoperable approach to Digital ID might emerge from formal standards processes. Governments are playing a role at the margins of these developments, but industry is plainly leading the way.

In order for major, market-clearing innovation in this field to occur, we anticipate that these multiple industry efforts will consolidate into one or a few at most. Consumers, increasingly given a role through user-centric models, may have a larger-than-ordinary voice in the outcome. It is unlikely that governments will have a central role in this consolidation process, though they are likely to play a part in ensuring that data protection laws are upheld and that competition can ensue after interoperability is accomplished, if it comes to pass.

Collaboration among industry leaders will be necessary in order to get the rest of the way towards an interoperable Digital ID system. Governments can help through soft regulatory approaches, such as bringing stakeholders together in dialogue and using their clout as major data holders and users. Interoperability and innovation in this environment will not come to pass through fiat of either major market players (as was attempted by Microsoft with Passport) or governments. This combination of industry efforts with a light-touch role for governments has the potential to lead to greater levels of interoperability in the Digital ID space. Once the technology becomes more mature, industry must find a way to attract consumer interest in order to cement demand both for Digital ID in general and interoperable ID platforms in particular.

Interoperability in Digital ID online has drawbacks that must be addressed, but has high potential to be generative as well. Digital ID interoperability could create new markets on at least two levels (competition for Digital ID itself and services built on top of a pervasive ID layer) and also enable interoperability among other applications and services. The incentives for market players are largely aligned at the moment, but may diverge as technological and market developments progress. The largest potential pitfall is a breakdown of collaboration among stakeholders. If those currently participating in the dialogue split off or throw support behind warring standards, user adoption will remain low, and little innovation will result. However, the current market trajectory is promising, and we should see significant innovation should user adoption ramp up.

APPENDIX

Computers interact with one another via the seven layers of the Open Systems Interconnection model (OSI), a framework that outlines the specifications, functions, and activities that occur in a computer network. The OSI model rests on the idea that the various tasks involved in communicating between two computers can be divided into distinct layers of related functions and activities. While many developers do not strictly adhere to the OSI model by keeping related functions in a clearly defined layer, the OSI model has been adopted as a standard by the ISO (International Organization for Standardization), and most networking products attempt to define themselves in relation to the OSI model.

Today's widespread use of computer networking has been enabled by the broad acceptance of protocols that define how computers will communicate with one another. Protocols are rules for communication (similar to languages) and they exist at each of the levels in the communication connection. It is protocols that actually implement the functions and activities detailed in the OSI layers.

When one computer sends data to another, the message begins its trip through the protocol stack at the Application Layer. The Application Layer is responsible for determining whether there are sufficient system resources on the sending computer to initiate communications. The Presentation Layer then ensures that the information will be sent in a format that is recognizable to the receiving machine. The Presentation Layer translates the data using the appropriate protocol so that it can be understood by an application on the receiving computer. The Presentation Layer is also the layer where data encryption or decryption is accomplished.

The Session Layer sends a service request establishing, and later terminating, communications between the two computers. The Session Layer is responsible for initiating the requests that will establish a communication connection between two computers. Once established, the Session Layer is responsible for managing and maintaining the communication session.

The Transport Layer is responsible for ensuring reliability and integrity of communications between two computers. TCP (Transport Control Protocol) is the protocol that controls most Internet communications at this layer. TCP divides the message into packets before passing them onto the Network Layer. The packets may take different paths to the receiving computer and will not necessarily arrive in the order sent. On the receiving computer, TCP reassembles the packets and requests that lost or damaged packets be resent.

Internet Protocol (IP) governs Internet communications at the Network Layer. Here, the addresses of the sending and receiving computers are added to the packet. A packet will wind its way to its final destination hopping from one computer to another. Computers along the way examine the addresses and decide where to direct the packet.

The Data Link Layer checks to see if any transmission errors occurred that changed the data inside the packet. It also manages communications within the internal networks of the respective sending and receiving computers.

The Physical Layer takes the packet and generates the actual electrical signals that will transfer information from one computer to another. Once these signals are received, the data is decoded and unpacked until it is usable at the Application Layer on the receiving machine.