Generating Revenue and Subscriber Benefits - An Analysis of:

The ARPU of Identity

THE OPEN IDENTITY EXCHANGE | PACIFICEAST RESEARCH

By Scott G R Rice

Table of Contents

The ARPU of Identity

1. Introduction

If you are familiar with the telco industry you know how to spell its favorite four letter word: ARPU, Average Revenue Per User. ARPU is a measure of monthly revenue divided by the total number of end-user customers. When ARPU is high, it means the telco has better customers--those that use lots of high margin services. When ARPU is low, the telco likely has the same fixed costs per user, and lower overall margin. In the minds of most telecom executives, ARPU going up is good, ARPU going down is bad. In this whitepaper we will review how and why telcos can and should play a stronger role in the identity industry. We will also provide a financial model for how various aspects of identity management can contribute to ARPU. Additionally, we will highlight some of the challenges facing the identity industry as a whole and some of the issues telcos will have to face as they navigate their way through the identity ecosystem.

As a backdrop to this discussion, it's important to start with the fact that mobile phones are rapidly reaching global ubiquity. In the next ten years it is likely that, on average, not only will every person on the planet have a mobile phone, but many will have more than one. That means almost everyone will have a smart, connected device from which to interact with all manner of online services anywhere they go, and increasingly have the challenge of proving they are who they say they are to those very same services from their mobile phones, tablets and desktops. In spite of the importance users place on these devices and the critical part they are beginning to play in our daily lives, the mobile network operators that bring life to these hunks of aluminum, plastic, silicon and glass must work hard to avoid falling into the dumb-pipe trap in which they facilitate consumer use of these devices but do not actively participate in the identity economy which protects users while allowing them to take on a safe, virtual identity required by so many useful and fun applications.

Ironically, many carriers fear becoming *just* a carrier. By this we mean that although the carrier is intimately involved in moving information from point A to point B, many carriers don't want to stop with just participating in that transport. They would also like to be a part of the content and the applications which function over the carrier's transport media. It is reasonable for telcos to fear becoming the identity industry's big, dumb pipe. They've made this mistake before.

In the mid 90's a new, consumer-friendly and fun concept called a "ring tone" started first in northern Europe then spread quickly across global markets. In those first 10 years of the ring tone golden age the market size rose from nothing to annual revenues of $500 million (US). In the beginning telcos were intimately involved in the distribution and production of ringtones. However, as the market size rose and as telcos began supporting downloads via SMS (even before internet-capable smart phones changed the actual distribution mechanism) the Over-The-Top (OTT) industry began and nearly completely subsumed the ring tone market. The telcos were not only left with very little of that $500 million in revenue, they had effectively paved the way for an OTT industry to take over the content market from them, leaving them only with a tiny fraction of revenue for being the distribution conduit. If telcos want to avoid painting their future selves into a dumb-pipe corner, they need to more quickly participate in nascent markets and actively work at maintaining a broader spectrum of services that support their subscriber base.

Unlike the telephone of the 90's, today's mobile device isn't just a way to call friends and family or order pizza delivery; it is a pivot point that connects our two existences. Our mobile phones have evolved to the position of a Carrollean looking glass: a portal through which our two worlds are connected: one digital and one physical. A mobile phone is the most logical connection between the physical and digital world because a phone number is the only universally established distinct, unique, global and mutually exclusive key which, just so happens, is connected to a piece of pervasive hardware carried around by almost everyone on the planet. Smart phones are ideally situated to bring physical identity and digital identity together.

Furthermore, in most cases, you don't just walk out of a mobile phone store with a $500 plus piece of hardware and access to virtually unlimited data and voice communications without going

through some form of credit check and the inherent identity verification that goes with it. Telecoms generally know who you are when you become a customer, which puts them in the enviable position as both supplier of a connected, smart device, and a verifier of identity (at least in part) to 3rd parties. Our phones, and hence the telcos that provide them, are ideally suited to have a significant role in identity systems because they serve as a simple, convenient, and pervasive connection between the physical and virtual worlds with which users interact.

Yet there is no more guarantee now than there was in the wild, early days of ringtones that the telecom industry will be a significant beneficiary of their strategic position. Social media companies are collecting a lot of consumer information including phone numbers. The absence of ubiquitous, authoritative identity systems will be filled … by someone. This paper will examine how the telcos are participating in the identity marketplace and what still must be done for them to maximize their role and revenue prospects.

2. Identity 101

Before diving more deeply into how telcos are involving themselves in the world of identity it is important to understand what the identity eco-system is and how the connections are made between our virtual identities and our physical identities. Understanding this is critical to understanding where Telecom fits into the picture.

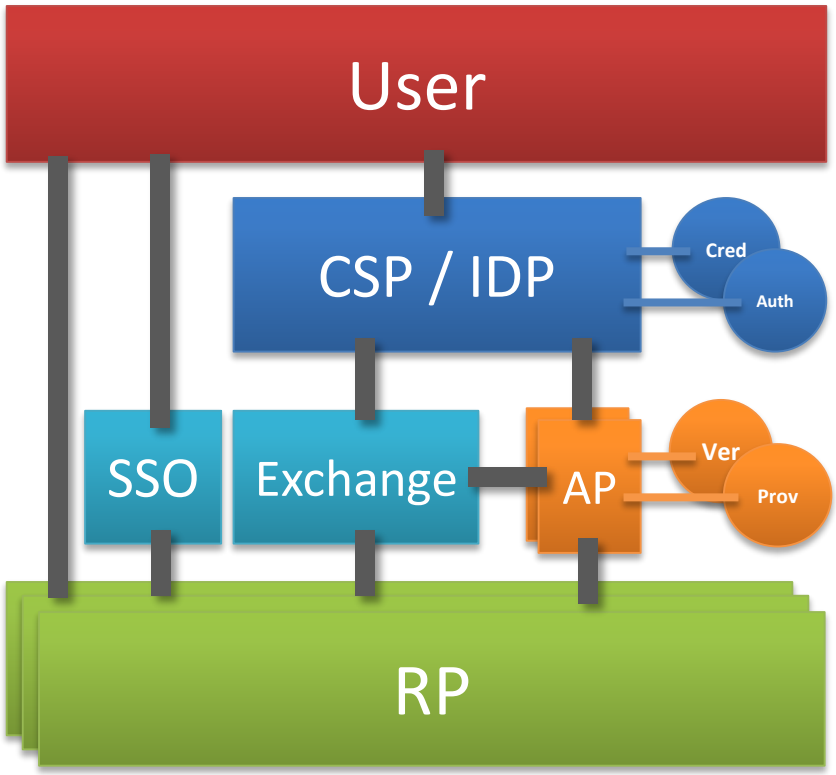
For the purposes of this discussion it is reasonable to divide the identity ecosystem into six interacting roles and four general transactions. The roles are:

Users – Individuals or physical entities who are the primary inter-actor with a virtual system. Users may interact directly with RPs, but could also go through SSOs or CSPs/IDPs in order to actually log in to an RP account.

SSO – Single Sign On – entities that integrate with multiple credentialing systems allowing users to access multiple accounts via a single credential.

CSP/IDP – Credential Service Providers or Identity Providers. These entities provide credentials to users and authenticate their subsequent access. CSPs/IDPs may provide second or multifactor factor authentication to enhance security associated with online access. They may also provide or broker identity attributes (acting as an AP).

Diagram 1: Common Interactions of Identity Roles



RP - Relying Party – entities that exchange physical products or services with virtual identities. RPs may interact directly with Users or may interact indirectly through CSPs. They may also choose to acquire or verify attributes directly through APs or work through Exchanges. They are called "relying parties" because they rely on identity providers for actual credential and authentication services.

Exchanges - entities that allow one or more RPs a single point of technical and contractual access to multiple CSPs/IDPs and attribute providers or verification systems. They may perform SSO functions and also have various identity blinding features to shield information about users from CSPs/IDPs (e.g. which RPs users are going to) or from RPs (e.g. which specific CSPs/IDPs represent a user). This latter functionality is important to help manage privacy and effectively implement a trust framework between all the parties. Exchanges may also perform commercial functions such as billing and settlements between all the parties as

a mechanism to simplify contractual arrangements. Some Exchanges also integrate with APs for access to data provisioning and consumer identity verification services.

AP - Attribute Providers – entities that provide access to information about Users or verify the information Users provide. RP's may interact directly with APs or they may work through Exchanges that give them access to multiple APs. A CSP/IDP may also act in the capacity of an AP if they have bundled authentication with identity attributes as part of an overall value proposition.

In addition to the noted interactions between each of the roles, the four general identity transactions are:

- Credentialing – assigning a virtual identity to a physical identity. Also known as "Registration".
- Authentication – verifying a user's access to an existing credential. Also known as "Logging On". [1]
- Verification – using a third party to confirm assertions a consumer makes about themselves
- Provisioning – using a third party to gain insight to more consumer information.

Users and RP's have been around since before the beginning of eCommerce. However, Exchanges and SSO providers are fairly recent additions to the identity ecosystem. Exchanges are essentially marketplaces of credentials that consumers already have and, where applicable, consumer

[1] There are two additional types of authentication worthy of note: Two-Factor Authentication and Biometrics. Authentication systems largely follow the token plus shared secret model. This means a user uses a particular token or ID to access a given system and is granted access as long as they prove to the authenticating system that they know the value of a secret known, theoretically, only to the authenticating system and the user. Simply put: a password. In most cases requiring higher levels of assurance an additional or second "factor" is used. Theoretically, the more factors used the less the chance that the wrong person will be allowed access to an account. However, the more factors used, the greater the user friction so easy to use second factors of authentication are often sought out. Currently the most common form of second factor authentication is a PIN sent to a cell phone via either an SMS message or a voice phone call using an interactive voice response (IVR) system. Another common form of second factor authentication (although it can also be used as a primary form of authentication) is biometrics. Biometric authentication includes fingerprint readers, iris scanners, even face and voice recognition. We won't go into details about these applications but it is helpful to know where they fit in the spectrum of authentication services.

information attributes from trusted 3rd parties (CSPs/IDPs/APs) that have previously enrolled these users into their respective services. Exchanges have a variety of benefits:

- For users, it increases convenience since they don't need to obtain yet another set of credentials and/or verify their identity with yet another service provider;
- For RPs, it reduces friction when a new user registers with their service (since this has already been done by a trusted 3rd party), increases the level of assurance that the user is who they say they are, and may also reduce fraud and account takeovers where CSPs/IDPs have adopted enhanced security measures such as multifactor authentication and/or biometrics to safeguard credentials from improper use.

While an RP can choose to interact with just a single AP or even integrate with multiple APs, the technical complexity of these multiple, concurrent interactions has created a value added reseller market that has come to be known as an "identity exchange". Just as Exchanges reduce the number of contracts and integrations RP's must maintain, SSOs allow a single user or an RP to access multiple credentialing systems via a single path. Exchanges and SSOs also enforce privacy and security policies, improving data safety while they reduce user friction.

3. Where Telcos Fit In

There are two primary areas in which telcos can and should play a role in identity: (1) as a credential service provider (CSP), leveraging the security capabilities of mobile devices anchored in telecom networks, and (2) as an attribute provider (AP), leveraging enrollment and account status information about a particular customer. Not coincidentally, these two areas are also the focus of the revenue enhancement model described in the next section.

David Pollington, the Senior Director of Technology with the GSMA (a global mobile technology industry group) leads GSMA's identity practice. He is one of the leading experts in telecom-centric identity systems. GSMA's leadership in telco identity initiatives has been seminal in drawing attention to the needs and opportunities of the identity markets and Pollington's role at GSMA places him in the middle of telecom-centric identity projects around the world. This

exposure gives him first-hand insight into the value of identity systems not only for telcos but for relying parties as well. "Identity services in general are underpinned by the need for the individual to authenticate themselves, to authorize transactions and to be able to give consent to attributes about their identity to be shared with RPs. At a basic level, this authentication mechanism can be monetised as a two factor authentication service without needing to pass any identity information to the RP."

Pollington outlined several areas in which GSMA's telco members are either already involved or actively investigating. "Telcos are in a strategically great position to supply intelligence in the form of verification of information RP's collect. Questions can be asked of these verification systems like 'does the user live in London', or 'what is the subscriber's name or gender', or even 'is this person old enough to purchase fireworks or alcohol'." Pollington stated that RP's are also very interested in reducing user friction and data entry. "With a consumer's consent, telcos could provide data used to fill out forms, especially on mobile devices. RP's gain value in other forms as well such as reducing KYC (know your customer) costs by leveraging verified attributes from another source and removing risk of prosecution by selling goods to under-age users".

GSMA believes its mobile network operator (MNO) members are well placed to provide services within an identity framework because:

- MNOs are regulated in many markets to register customers (KYC) and protect minors
- MNOs verify identities as part of the contract provisioning process
- MNOs are able to verify identities face-face through their retail chains

In addition to the verified socio-demographic information that MNOs have on their customers they can also provide other static and dynamic attributes – for example, location - verifying that a user's mobile phone is in proximity to a point-of-sale terminal or ATM where the user is making a transaction. Most importantly MNOs providing such services do so in an open and transparent way that protects user privacy and ensures users have control over how their attributes are used. An excellent additional reference on the topic is a GSMA presentation called "Introducing Smart Solutions" ***[GSMA[1]].***

As an attribute provider and exchange that actively works with many of the largest telcos in the US and Canada, PacificEast also sees a hungry market for four primary types of telco related transactions:

- Consumer Verification – receiving name and address from RP's and verifying it against subscriber billing address information or other third party data sources.
- Active/Inactive Verification – confirmation if a phone number is active. These checks may be used to keep customer and membership contact files clean or to avoid wasting time and resources calling disconnected numbers.
- Account Type checks – many risk mitigation specialists believe there is a higher level of fraud when a transaction is associated to a pre-paid account than a post-paid (contract) account. Anonymous telephone numbers (like those from Tracfone or through VoIP services like Google Voice are believed to have a higher incidence of fraud. Retailers frequently ask for this kind of account-type information to integrate into their fraud scoring models in order to better predict risk associated to online orders.
- Compliance Checks – different compliance regimes and regulations affect many aspects of making outbound calls. In the US, the Telephone Consumer Protection Act (TCPA) includes different rules for handling wireless versus landline phones. TCPA compliance also requires information about where the phone is located so the time-zone can be used to comply with time-of-day limitations and even whether or not a telephone is registered to a consumer or a business. All this information has to come from somewhere and the telco is the best, most authoritative source of these simple attributes.

We know telcos can be attribute providers; some already are. We also know telcos can be credential providers; some already are. The question is not if it is possible but if it is practical. That practicality has a lot to do with the revenue they can expect from introducing these new services. In the following section we will assess the revenue potential when telcos participate in one or more identity roles.

4. Identity's Impact on ARPU

Recently there have been various industry recommendations to switch from ARPU, average revenue per user, to ARPA, average revenue per account. ARPU is inherently focused on an individual using telco services. But device penetration rates exceeding 100% indicate individual users are carrying multiple devices; each device could have a different type of plan (for example pre-paid versus post-paid) and different data rates as well. This complexity can confuse what ARPU means to carriers, hence the consideration of a switch to ARPA as a primary measure of unitized revenue. ***[Eurocomms]***

Yet, according to Robert Blumenthal, EVP of Marketing and Business Development at SecureKey Technologies, ARPU is very much alive and well in the minds of telecom executives. "Maintaining ARPU is a constant focus in telecom. There are many factors like churn that can drag ARPU down so telcos are always on the lookout for new ideas and strategies that move ARPU back in the right direction. When you have millions of subscribers, raising ARPU by just one penny a month can have a big multiplier effect. That single penny increase in ARPU for an MNO with 50 million subscribers adds six million dollars to the company's annual revenue. Even for a company with annual revenues in the billions, these amounts are noticed since they go right to the bottom line."

Blumenthal should know. Before taking up the identity challenge at SecureKey, he was a 25-year veteran of telecom, most recently as President of Virgin Mobile Canada. He says "the telco exec has within his psyche this goal of 'revenue annuity'; they want to see regular recurring revenue". Thus far ARPU has been the measurement de rigueur.

SecureKey hasn't been around that long (established in 2008) but they are having an impact on the identity ecosystem markets and have become a major player in government identity initiatives in both the US and Canada. In 2011, SecureKey won a major bid for the Canadian government that enabled banks to be credential providers for citizens who wish to access government services. The service went live in 2012 under the brand "SecureKey Concierge" and has attracted a significant number of online users, all within an umbrella of privacy and security. Similarly, SecureKey also

won the bid for the US government's Federal Cloud Credential Exchange, or FCCX, project (nicknamed "F6" and Connect.gov) in 2013 which will see the US Postal Service become a central identity broker for various federal governmental agencies. SecureKey's ***briidge.net Exchange*** product is a major component of the USPS's hub topology as well as Canada's SecureKey Concierge service.

SecureKey's briidge.net Exchange service was initially designed to use online and card-based contactless banking credentials to access government services. However, it is now growing to support citizen and consumer access into other levels of government (provincial/state and municipal) as well as for private sector services. It is also working with Canada's major telecoms to enroll them as credential providers which it believes will provide greater market coverage and additional choice and convenience for consumers. The task of establishing relationships with all the banks and all the telcos is made somewhat easier in Canada with only a half dozen banks, three major telecoms, a single federal government and a dozen regional/provincial governments. However, even with relatively few entities it was no small feat to address legal, regulatory, technology and commercial issues in a multi-party identity ecosystem to everyone's satisfaction. The US, for example, would be significantly more complex by virtue of the hundreds of potential identity providers in the form of banks and telecoms, the hundreds of government agencies across a wide spectrum of federal, state and local jurisdictions and the significantly larger size of its private sector. However, even with the additional complexity, the same underlying model seems a reasonable way forward.

But even in a market with hundreds of potential RPs--or maybe because of that--telcos have a great opportunity to play a significant role in identity provisioning and verification because of their reach and penetration in virtually every market around the world. In fact the penetration rate in the developed world exceeded 100% in 2007 meaning, on average, not only does everyone in the developed world have a phone, many people have more than one. ***[ITU]*** Even outside the developed world, cellular device penetration rates are nearing 100%.

In Africa, where brick and mortar banks aren't available to large portions of the population, cell phones stand in as a remote banking tool. This crucial service they provide has pushed mobile

penetration rates close to 70%. In developing countries (significantly more than in developed countries) people use their cell phones to pay for goods, pay bills, and even get access to cash. The global nature of the telephone and its near ubiquity make telecommunication providers an obvious choice for providing authoritative identity services and credentialing.[2] ***[GSMA[2]]***

5. The ARPU of Identity: A Working Model

Among other things, Blumenthal's role at SecureKey is to convince telcos to participate in identity projects. As a seasoned telecom executive used to being on the "buy" side of the table, he isn't just using words. SecureKey has developed a financial model as a means to support these arguments - a large, fairly detailed spreadsheet that he uses to calculate revenue potential over the next few years from multiple types of identity projects. The model quantifies what has been difficult to pin down up until now: the potential identity-centric revenue impact for the telcos articulated as monthly ARPU Contribution; i.e., the Average Revenue Per User for Identity, or ARPU-I. SecureKey has granted the Open Identity Exchange the right to publish an open source version of their model and to include its details in this white paper. The OIX ARPU-I Model is available as a working spreadsheet on the OIX website.

As the "how do you eat an elephant" joke suggests, the elephantine ARPU-I Model must be digested one bite at a time. The model breaks the identity market down into five segments of potential customers, or RPs:

- Federal Government
- Regional & State Government
- Healthcare
- Utilities
- Retail & Private Sector

[2] Editor's Note: The referenced document from the GSMA is an excellent follow on document if you would like to dive more deeply into economic opportunities for MNOs.

Within each of these five RP sectors the number of participants and estimated amount of use for each participant in each sector is estimated over the next five years. Revenue estimates per type of identity transaction (authentication versus attributes) rounds out the model and allows future revenues to be projected. For modeling purposes, these are "educated" estimates, but may vary from market to market over time and among different applications. Finally, the model divides those future revenues amongst the various participants in a given identity process. The model categorizes most identity processes into those relevant for providing identity credentials (IDP/CSP services) and those relevant for verifying or providing identity attributes (AP services). This is particularly useful for calculating ARPU-I because not all telcos would likely participate actively in both types of processes.

The difference between credentialing/authentication activities and attribute activities merits a simple example. To make a purchase online a user first registers for an account. In the identity field, that original registration process is called credentialing because a digital key (the credential) is assigned to a physical person. The subsequent process of logging in after registration is called authentication since the user's attempt to use the key to gain access to an account must be authenticated. Finally, the information exchanged between the user and the RP (called user assertions) and the RP and third parties (who either verify the consumer's assertions or provide more information) constitute the attribute transactions that continue to occur over the life of an account. While the full ARPU-I Model is very detailed and includes projections for a 5 year period, for simplicity of explanation just a single year has been extracted for the example in Table 1, below. Assumptions regarding the average number of Relying Parties per user, percent of penetration of active users of services within a given industry sector, and other factors are highlighted.

The model begins by estimating how many credentials would be likely for a given population. In this example the US is used but simply changing the market area's demographics will adjust the model appropriately for other countries. The total population of 320 million is reduced by the number of minors into an available population. For each of the five sectors a market penetration is estimated which equates to how many of the available population a particular market is likely

to serve as well as how many credentials or accounts a given individual is likely to have in that sector. For example, a person is likely to have only one federal account but may have two credentials at the state or county level for their driver's license and their state income or property taxes. That same user could have separate credentials for their medical insurance and their dental

Table 1 – A One Year Example of the OIX Average Identity Revenue Per User, or ARPU-I.

Summary						
Year	Market	Pop (000)	% over 18	TAM (000)		
2016	**US**	**319,160**	**77%**	**245,753**		
Market Size by Sector	**Federal Gov**	**Regional Gov**	**Health Care**	**Utilities**	**Retail & Private**	**Total**
Market Penetration by Sector	63%	80%	47%	47%	80%	
Total Available Market Users (000)	154,824	196,602	115,504	115,504	196,602	
Average RP's per User Per Sector	**1**	**2**	**2**	**3**	**10**	
Total Credentials (000)	154,824	393,205	231,008	346,512	1,966,024	3,091,573
Est. Sector Active User Adoption Rate (%)	**10%**	**5%**	**5%**	**5%**	**5%**	
Est. Active User Credentials (000)	15,482	19,660	11,550	17,326	98,301	162,320
Average Annual Identity Transactions	**2**	**3**	**4**	**4**	**15**	28
% of Trans. Requesting Attributes	**70%**	**70%**	**80%**	**40%**	**40%**	
Total Credentialing Requests (000)	30,965	58,981	46,202	69,302	1,474,518	1,679,968
Total Attribute Requests (000)	21,675	41,287	36,961	27,721	589,807	717,451
Revenue Potential by Sector						
Assumed LOA Minimum Requirement	2	2	3	2	1.5	
Annual Auth. Subscription per Credential	**$1.80**	**$1.40**	**$2.80**	**$0.80**	**$0.20**	
Annual Credentialing Revenue ($000)	27,868	27,524	32,341	13,860	19,660	121,255
Revenue per Attribute Transaction	**$2.00**	**$2.00**	**$5.00**	**$2.00**	**$2.00**	
Annual Attribute Revenue ($000)	43,351	82,573	184,806	55,442	1,179,614	1,545,786
Credentialing & Attribute Totals ($000)	**71,219**	**110,097**	**217,147**	**69,302**	**1,199,275**	**1,667,041**
Annual RP Cost Estimates	**Federal Gov**	**Regional Gov**	**Health Care**	**Utilities**	**Retail & Private**	
Avg. Cost per User Credential (Auth. & Attributes)	$4.60	$5.60	$18.80	$4.00	$12.20	

insurance and any number of accounts for their various utilities (phone, cable, electric, gas) and possibly a dozen or more credentials for the rest of their digital identity including bank access and

online shopping accounts. All those credentials related to a given individual are aggregated into a total credential count. The model then makes allowance for the fact that not all individuals are going to be active so an active percentage by sector is estimated, the product of which is a total number of active credentials.

Each credential is presumed to be associated to a given number of login activities and subsequent attribute exchange or verification activities. At this point the model makes an important assumption about the likely difference between the business model for credentialing and the business model for attributes. The ARPU-I Model assumes that credentialing activities are likely to follow a subscription model (a given annual rate per credential) and that attribute activities will follow a transactional model (a given cost per attribute per transaction). The model allocates different estimated costs which an RP would pay per credential or set of attributes based on the RP's industry sector. For example, the Federal Government might pay $1.80 per credential per year to a credentialing service provider (CSP) but a Healthcare company may pay $2.80. It is a reasonable assumption that different industry sectors will pay different rates for the same activity because of either volume differences or differences in the level of assurance, or LOA, for a particular credential. (Because of the sensitivity of healthcare information the LOA is assumed to be higher than what is needed to check, say, utility usage. A higher LOA would equate to a higher cost to protect the credential.)

Finally, the model applies some revenue estimates for each attribute transaction. These estimates are an average of all the various types of attribute transactions that might be needed. For example, a credit score and history from a credit bureau might be $20 or more, but a single address verification check may only be a few cents. There might be room here to break down the attribute charge estimates into more detail, but this average is a reasonable simplification for an already complex model.

When all is said and done, assuming the underlying assumptions in the ARPU-I Model are at least conservative enough to be believable, there is significant opportunity in identity for telecoms. This simple market example yields a $1.6 billion market opportunity in the US with only about a five

percent penetration of users in a handful of applications. There is also potential upside as well with an estimated growth to $8B per year or more with increased market penetration.

Table 2 – ARPU Contribution due to Identity or "ARPU-I" for the 1 Year Example.

ARPU Contribution / ARPU-I	Credentialing / Authentication Only	Attributes Only	Both (Total)
Total Annual Revenue (000)	**$121,255**	**$1,545,786**	**$1,667,041**
Revenue Per Active User Credential	$0.75	$9.52	$10.27
Monthly Rev. per Active User Credential	$0.06	$0.79	$0.86
Monthly Identity Related ARPU Contribution (ARPU-I)	**$0.04**	**$0.52**	**$0.57**

These specifics are detailed in the companion spreadsheet to this paper. A large part of the value are real-time, verified user attributes rather than pure authentication. Nonetheless, both are important in the context of providing higher levels of assurance regarding consumer and citizen identities.

GSMA's Pollington agrees with this latter point stating that the chief value in the ARPU of Identity will be driven by the supply of verified information. "This information may be provided in a raw state (e.g., DOB) or in the form of intelligence (e.g. 'is this person old enough in this jurisdiction to purchase fireworks?"). GMSA sees a significant role for telcos in not only being the conduit through which this verified information can flow, but also as sources for the information itself."

As a means of calculating market potential the ARPU-I Model factors in all the necessary points. It provides a much needed way to break apart the various aspects of the identity market into smaller pieces that can be assessed and refined independently.

6. Current Commercial and Government Activities

The telecom industry still has a way to go to reach the critical mass of consumer data and service coverage needed by the identity industry. However, progress is being made. Often, as would be expected, the fiercely competitive wireless telcos see these services to their subscribers as a

competitive advantage. But there are times when the common good brings these competitors together on behalf of all subscribers.

One of those times was in 2010 when the Open Identity Exchange sponsored the creation of an industry-wide working group focused on developing a trust framework centered on telecom-centric identity verification. Over the subsequent three years heavy hitters like AT&T and Verizon worked side-by-side to establish a set of principles, policies and rules which governed how the telcos would agree to provide consumer identity verification services. The author, as a representative of relying party concerns and as a neutral third party, was asked to chair that working group which published its final framework in the spring of 2013. ***[OIX]***

Participating in identity ventures among the telcos continues to develop. Verizon has also been a significant player in providing credentialing services and is, in fact, the only telecommunications company certified under the Federal Identity, Credential and Access Management (FICAM) program to provide the most secure Level of Assurance (LOA) credential, Level 4. ***[IDManagement]***

AT&T, Sprint and TMobile have not yet produced significant credentialing services nor do we know if that is in their plans, but there are signs they may be investing in attribute verification systems that help reduce fraud against their subscriber base and could, once integrated into eCommerce identity verification systems, be used to help subscribers lacking significant credit histories establish and verify their identities and build up a more established profile for which, traditionally, they would have needed the credit industry to do for them. In other areas telcos have acted more independently, mapping out their own course but, in the process, providing good examples of how identity-centric initiatives can be valuable to their bottom lines.[3]

[3] Rogers, the largest telecom company in Canada and a major investor in SecureKey, last year also invested $7 million US in TRUSTID, a technology startup providing a form of identity fraud prevention to the banking industry. When customers call in to activate their bank cards, the bank's IVR used to look just at the incoming phone number, cross referencing it against the phone number on file for the account associated to the card. However, fraudsters quickly figured out they could steal banks cards from the mail, lookup the phone number for the victim and run a cheap software program that calls the bank's activation line but transmits the victim's phone number instead of theirs. This has become known as Caller-ID spoofing. TRUSTID's platform prevents this identity fraud by assessing subtle details within the phone network itself. Since banks are not generally experts at telecommunication network analysis, they are signing up TRUSTID to shut off this particular fraud vector. OIX is scheduled to publish a paper this fall with a more detailed analysis of Caller-ID spoofing.

There are a few new public/private partnership pilot projects that bear mention. Below are listed several upcoming pilots, new standards that will affect telecom related identity initiatives, and a summary of upcoming activities in the US, Canadian and UK markets.

- The US National Strategy for Trusted Identity in Cyberspace (NSTIC) has just announced a grant of over $800,000 to support a GSMA pilot of a mobile-centric identity project with the four major US mobile network operators. ***[NSTIC].***
- Banks in the US, UK and Canada will be announcing new mobile identity pilot projects testing new Internet identity business models utilizing hubs or exchanges to increase security, privacy and ease-of-use. ***[AmericanBanker]***
- The OASIS Electronic Identity Trust Elevation Methods Technical Committee will help align the finalization of its standards development processes with pilots in the US, UK and EU to provide for "step-up" authentication at various levels of assurance. ***[Oasis]***

The success of programs and procurements like the UK's IDAP and the US's FCCX rely on public and private sector collaboration and development of open identity standards for trust elevation, single-sign-on, user consent and permissioning optimized for the mobile device.

The Open Identity Exchange is active in several new telco/identity initiatives.

- The Open Identity Exchange, the OpenID Foundation, OASIS, CTIA and the GSMA will help coordinate pilots and standards development activities in the US, UK and Canadian pilots. These industry non-profits are well positioned to optimize public/private partnerships focused on identity.
- OIX and GSMA plan a series of workshops on "privacy engineering" to ensure privacy by design principles are embedded in pilot discovery projects and that concepts and standards of privacy include allowances for federation and interoperability. At these workshops, privacy and consent will be considered not just in terms of how a single RP or IDP implements the concepts, but also how privacy and user consent can be made interoperable and transportable from one RP/IDP to another.

- The NSTIC International Coordination Committee, the Digital ID and Authentication Council of Canada, or DIACC, and the UK Identity Steering Group will help coordinate and publish lessons learned.

7. Challenges

Progress is being made and an identity ecosystem is being formed that is proving to be a potentially advantageous channel for the telecommunications sector. However, there is more work to do and several significant challenges that could yet derail progress or, at the very least, slow it down. In the following pages some of the known challenges have been divided into sections related to data coverage, consumer consent, finding relying parties and thinking through potentially new forms of technology.

Coverage & Quality

Telecommunication companies that want to participate in either a CSP market (providing login or credentialing services) or in an Attribute market need to remember they are not the first to the party. There are other established players in both markets and although the total market place is growing, telecommunication providers need to be able to compete in several areas if they want to be successful. The area in which competition is most important is data coverage.

For RP's to be convinced to modify their systems to rely on telcos for important consumer information, the RP needs a minimum level of critical mass of coverage. This minimum critical mass will always be larger than a single telco. No single telco has enough information to compete as an attribute provider against existing competitors in the market. Although telcos have some specific data attributes which cannot be replicated by traditional consumer information brokers, RPs are reticent to invest in any system that will only provide the information they need less than 70 to 80% of the time. Telcos, especially MNOs, may not relish cooperating with their competitors but the consumer attribute market, like the fraud prevention services market, requires cooperation.

MNOs especially need to understand that these markets are completely unlike their native, zero-sum market for minutes and bytes. No carrier can supply information for all consumers so cooperating with "the other guys" is paramount to success. As more telcos participate in these services, the critical mass of available data and ubiquitous service increases. As the critical mass increases, the market's effectiveness and competitiveness with non-telco alternatives increases. As the telco market increases, the revenue availability for each telco will increase. Therefore, as more telcos participate, each telco makes more money, not less. It is understandable that this "inverse competition" is a particular economic formula that does not come naturally to the telco psyche, but it is critical for telcos to appreciate that success in the identity market is not driven by the same factors as their native markets.

Platform providers, like SecureKey's Exchange and PacificEast's Telified have gained market share by integrating other non-telco data sources into their systems. (SecureKey also uses banking credentials in their credentialing system; PacificEast gives its customers the choice of verifying identities against credit bureau records when a telco record isn't available.) However, both providers are actively integrating telcos into their respective platforms. The key challenge is that of coverage ubiquity. Some telcos just may not want to be involved, or the ARPU estimates, especially for smaller telcos, may not be significant enough for them to prioritize participation.

But coverage isn't the only data related challenge to telco participation. In the US the highest quality consumer subscriber data has significant disclosure limitations so platforms that use it often have to support only verification that a consumer's asserted identity matches what the telco has on file. On the surface that might sound like a simple enough task, but few telcos have the in-house expertise for specialized consumer-data comparison processing which is more typically found in data management companies and data brokers. These latter types of companies are the likely competitors for the telcos in this consumer verification market.

Within the telco data itself, there are also challenges, especially in markets with high percentages of pre-paid, family-plan, or corporate users. Pre-paid phone accounts, for example, usually don't require credit checks or identity verification when signing up. They often don't have contracts and are, in some cases, virtually anonymous. Similarly, users within family plans or corporate

accounts may not be known to the telco by name. The result is a lack of means of verifying the consumer information associated to some phone numbers. On the surface that may not sound like a bad thing. However, consider what would happen if law enforcement could only find authoritative information about half of all drivers' licenses, leaving the other half undocumented but half of those undocumented licenses completely legitimate. The result would be that only some licenses could be definitely verified and it would be impossible to verify that a given license was not valid since not all valid licenses were known. Ideally, telco identity verification should be able to detect not only when an identity assertion is valid, but also when it is wrong. This might require a separate enrollment process for "anonymous" individuals outside the normal telco activation process if they want to participate in and take advantage of the identity services their telco can offer.

There are similar issues with other types of anonymous phone accounts provided by companies like TracFone and Level 3. TracFone and other "burner phone" carriers supply pre-paid (often paid for in cash) mobile phones which are completely anonymous. Level 3 is a major US provider of VoIP phone numbers for free phone services like Google's Voice platform. These phones are not only anonymous but in most cases, because Level 3 numbers are also used for legitimate VoIP and business phone systems, the burner numbers and numbers for legitimate business needs are intermixed, unidentifiable and indistinguishable.

Apps like Burner (www.burnerapp.com) provide another way to use temporary phone numbers and then "burn" them at which point they are recycled back into their number pool. Burner's public claim is that these phone numbers are ideal to be "*given out as a temporary number that can be deep-sixed at the very moment your blind date gets awkward"* ***[BurnerApp].*** But according to Bruce Schneier, a blogger and expert on technology and security, law enforcement finds these kinds of burner phones and apps interesting enough to invest in a means fingerprinting them in order to separate the burner phones from the rest of the pack. ***[Schneier]***

These challenges all add up to somewhat reduce the quality of any phone-number centric identity verification system. However, this is a case where more carrier openness and involvement can actually improve the use of telephones for legitimate commercial purposes and reduce the value

of the phone as a means of conducting illegal activities. Challenges with data quality are found in any information source, but Blumenthal suggests that, over time, the carrier might want to consider working with experts in the data business that can help them improve their data quality and quantity, which could, in turn, increase the value of their own information in the broader marketplace. As an example, PacificEast actively works with telcos to supply expertise in name and address matching to help carriers provide better quality identity verification without having to build it themselves.

Consumer Consent

In many identity ecosystem transactions not all parties have a direct relationship with the user. Without direct user access, for example, the AP must rely on the RP to collect a consumer's consent for accessing or verifying their data. When the AP is a telco and the telco's existing terms and conditions agreement with the subscriber doesn't already allow this particular use of the subscriber's data, how does the telco get permission from the user to perform this work? The only option, in this example, is to pass the consent through the RP which has contact with the subscriber. That requires the RP to collect not just the consent *their* legal department requires, but the consent required by the particular telco as well. What if the parameters of the consent (for example, the period of time for which the consent is valid) don't match between what the RP collects and the telco requires? This scenario isn't really that unlikely and it highlights the difficulty and complexity for all parties (including the user) of authorizing every party in a transactional chain. This is one of the greatest difficulties in these complex transactions because all parties to the transaction, the RP and the AP and possibly also an Exchange, have different legal requirements and expectations for release of information. This situation quickly becomes an interoperability nightmare driven by outdated notice and consent laws.

Notice and consent laws have been around for years. The Organization for Economic Co-operation and Development, or OECD, first published their seminal seven Privacy Guidelines in 1980. ***[OECD]*** However, those were simpler times with much less technology. There wasn't a world wide web or even a cell phone. In the US, AT&T wasn't "a" phone company; it was "the" phone company. Credit bureaus as we know them today didn't exist yet; there were no big data brokers

collecting thousands of data points on hundreds of millions of individuals. What privacy laws needed to protect back then was very different than what they need to protect today. Yet the OECD guidelines haven't substantially changed in the last 34 years. Needless to say, privacy laws and, specifically, the notice and consent requirements of those laws are insufficient for today's technology and the business needs that are driving that technology.

In 2013 (and updated in March of this year), Microsoft and Oxford University's Oxford Internet Institute (OII) published a report outlining recommendations for revising the 1980 OECD Guidelines. Their report makes clear recommendations for rethinking how consent should be managed in the internet age. In the report's forward, Scott Charney, Microsoft's Corporate Vice President of Trustworthy Computing stated "if the goals that informed the 1980 OECD Guidelines are to have meaning in the 21st century, we must ensure that fair information principles can still be applied effectively. It will not be enough to hold on to old paradigms, such as heavy reliance on notice and choice". ***[Cate]*** The report makes the point that expecting data subjects to manage all the notice and consent duties of their digital lives in circa 2014 is unrealistic at best. The report quoted a 2008 study published by Ohio State University that claimed "reading the privacy policies of just the most popular websites would take an individual 244 hours—or more than 30 full working days—each year." ***[McDonald]***

Some of these recommendations are controversial, but the obvious alternative is to continue to move toward direct consumer control over all data usage. As privacy-centric as it may appear on the surface to enable direct consumer control over information in which they are the subject, the burden of responsibility that level of control places on consumers is unreasonable due to the amount of effort it would take for consumers to perform each of these tasks. That, of course, assumes consumers or data subjects understand the context to which that consent and control applies and the implications to their lives for each decision they make.

The OII report recommends reversing the current trend of shifting the responsibility for data protection onto the data subject to a new series of data and privacy protections aimed at controlling and limiting disclosure and placing responsibility on data users. This privacy schema is not unlike that laid out in the US in the Graham Leach Bliley Act, or GLBA. ***[GLBA]*** Privacy controls in

GLBA are targeted primarily at controlling disclosure of data sourced from any kind of financial record and there are exemptions for particular uses the government felt were reasonable and in the best interest of the consumer. The most important factor in these suggestions is that they recommend moving away from notice and consent because data subjects simply can't individually read all those notices and make all those decisions, at least not in the fully informed manner in which they should be made.

An absence of cohesive and practical consumer consent controls may not prevent advancement in identity management in general, but until a solution to the current mire of consumer consent policies and regulations materializes, any system, telco or not, that uses identity will, of necessity, need to be much more complicated than necessary. Interoperability of such systems will be complex and likely tend toward proprietary rather than standard interfaces.

Where Are the Relying Parties?

While this whitepaper has focused on telecom industry's potential as a credentialing service or attribute provider, there is another role within the identity ecosystem that requires particular attention and analysis. This role doesn't affect telcos directly but has become a limitation to the entire identity ecosystem, regardless of which kind of company is supplying credentialing or attributes. The role causing the most consternation in identity circles is the relying party.

In the current way the identity ecosystem is structured RPs are the entities that end up footing the bill. Identity Providers like CSPs and IDPs and attribute providers of all types, as well as exchange services and even SSO providers are all on the receiving end of revenue related to identity transactions. The revenue introduced into the ecosystem would have to come from the RPs yet RPs have been the least involved in the identity ecosystem discussions and working groups. Many in the identity field have wondered why that is.

To answer that question it is helpful to assess the identity marketplace from the RP's perspective and see what they see. The heart of the problem is that the identity community has a tendency to come up with solutions that, although they provide a wonderful convenience for consumers, forget three important assumptions:

1. They require the RP (often a for-profit business) to effectively finance a solution that primarily benefits another entity (the user)

2. They are ***not*** asking the entity (the user) who is receiving most of the benefit to pay for it because users, in this case usually consumers, do not like to pay for services they deem unnecessary.

3. Most consumers will not understand the value of identity protection necessary until theirs' has been compromised.

The challenge of the missing RP is similar to the consumer consent challenge because in both cases tasks are being delegated to the entity least equipped to perform them. Consumers are expected to read hundreds of pages of terms and conditions documents each year and instinctively know the context and extent of each permission request they received from RPs and APs. (In reality this isn't the expectation at all since it is well known that users will just scroll to the bottom and click "I accept". This is the core of our assertion that notice and consent doesn't really provide any security for users.) Likewise RP's are expected to pay their developers to remove their in-house and effectively free authentication systems and replace them with authentication systems for which they will then have to pay.

SecureKey's Blumenthal contends this failing is due to the fact that the identity industry tries to target the RP's technology and compliance people instead of the RP role that is most concerned with customer experience, the Chief Marketing Officer (CMO). Blumenthal states, "it is the CMO that is responsible for improving the customer experience. The CFO may want reduced costs and the General Counsel may want reduced liability and better indemnification, but the CMO is the person who is going to jump up and down for a better customer experience." Ultimately, the primary goal of integrating identity services is to improve customer experience. Reductions in risk and fraud rates are positive outcomes as is the increased insight into the customer that can come with acquiring data attributes. At the end of the day the RP's primary motivation for implementing new identity systems is to improve the experience for the RP's customer. The importance of outlining the RP's motivations is worthy of a further whitepaper just on that subject alone.

New Technologies. New Answers.

MNOs are accustomed to managing data transactions within their existing network infrastructure. Their subscribers are constantly downloading applications and ringtones to their devices, some of which may need to be added to the subscriber's bill. But these types of transactions are routed within the bounds of the MNO's networks via their own devices. Many identity transactions supporting authentication or attribute verification queries are much more likely to come from outside the telco's own network. Some carriers refer to these externally sourced transactions as off-board or off-portal transactions.

External transactions force telcos to support new systems and communication protocols. All tier one (and most tier two) carriers already handle external billing transactions either directly or through billing service providers. Identity transactions will not usually update a telco's billing system, but they may very well be reading information from it. These read-only queries for identity or attribute transactions are often structured in the form of a question and answer. Because these "query and response transactions" have to provide information to the non-telco world, the communication protocol is less likely to be their native SS7 signaling protocol and more likely based on TCP/IP and using a data transfer protocol of either Simple Object Access Protocol (SOAP) or the current favorite flavor of data transaction protocol, Representational State Transfer (REST). Regardless of the transactional protocol, these services are a means of external organizations asking them a fairly simple question and receiving back a structured answer. Telco product managers should keep in mind this simple question/answer protocol when extending their existing systems (or even building new services) to support identity transactions. Actual protocol aside, example questions and answers might look like this:

Question: Is "this" credential the one you have on file for "this phone number"?
Answer: Yes/No

Question: A person who claims to be your subscriber says their phone number is "this" and their name and address is "this". Are they telling me the truth?
Answer: Yes/No or, perhaps, the name is correct but the address is not.

What may seem to a telco to be a simple piece of truth or verification can be a remarkably valuable tool in preventing fraud and assisting subscribers as they interact in the digital world. However, it is important for telcos to remember that although the quality of their answers might be very good, there are other companies already established in this "answer" market. Credit bureaus and data aggregators are well established data providers and such answers have an already-established price point. Social media and search companies like Facebook and Google are also well established in the credentialing and authentication market.

It may, at first glance, not seem like a good business strategy for telcos to start into an established market. But telcos have an advantage in the quality of their information and their close relationship with the consumer while credit bureaus and data aggregators have only an indirect relationship. A telco's ability to interact directly with the consumer allows them to build and maintain a relationship of trust and to assist the consumer by providing direct benefits like identity verification and preventing fraudulent activities on their account. While telcos should take the existing competition seriously, they should also remember they have an advantage over much of the competition because of the nature of their direct consumer relationship.

8. Conclusions & Recommendations

Participation in identity, especially as a means for subscribers to prove they have an established account and payment history provides an important value to the subscriber. A telco that provides the subscriber with tools to make their online experiences more rewarding and less painful, whether conducted on a mobile phone or on their desktop, should expect to earn subscriber loyalty. Subscriber loyalty reduces churn and churn is a significant source of operating cost and margin loss, since in order to maintain the same number of customers with the same revenue, telcos would have to invest more in adding new customers in order to offset the loss of existing customers. Churn reduction can be as valuable to telcos as revenue or ARPU enhancement since it goes right to the bottom line in terms of operating margin.

The ARPU-I Model is an effective method for telcos to predict their revenue from participating in the various parts of the identity industry. And while ARPU-I will never overshadow the ARPU from voice and data plans, it can provide lift when so many other factors are constantly pulling ARPU down. The Model, however, does not account for the churn benefit associated with making a subscriber's telco identity as indispensable in the virtual world as their mobile phone already is in their physical world. Although this is intuitive and potentially considerable, it is not yet easily quantifiable.

Specific to the attribute market, telcos have a lot to commend. They provide the only globally unique identifiers which can be used by a consumer to cross between their virtual, online world and their physical world. In many cases they have high quality information (like billing and service addresses) that have the benefit of being updated each time the subscriber pays their bill. Telcos are also, at their core, technology companies.

One of the biggest challenges telcos face is their lack of comfort with the concept of inverse competition. It does not come naturally to the zero-sum view that telcos, especially MNOs, have of competition; i.e., "If I obtain a subscriber, I am preventing my competitor from obtaining that subscriber". Telcos need to think of their participation in fraud-prevention and identity verification programs as a cooperative venture in which each party receives more benefit from cooperation than they would if acting independently. The identity market has a federated economy of scale that is very different from the zero-sum market for minutes, data and devices.

Finally, there is room for better regulation and/or industry practice especially around effective handling of consumer consent and privacy. Technology is scalable. Humans are not. As technology increases the flow of personal data, humans will not be able to manage the increasing number of consent requests nor understand how their consent (or refusal) will affect either the privacy of their personal information or their ability to conduct commerce online. If the only indemnification available for businesses providing identity services is either from consumer consent or from regulatory exemptions, and if regulatory exemption is spotty and haphazard, then credentialing and attribute providers will have the onerous, and often user-unfriendly task, of capturing detailed consumer consent during every transaction. Continuing to use the traditional

notice and consent mechanisms for an upwardly spiraling volume of transactions will lead to an untenable increase in consent requests that would eventually implode under its own weight and unwieldiness.

We must rethink how consumer privacy can be protected without relying solely on consumers to take on the full responsibility. Consumers have an obvious interest and significant stake in what happens to the data of which they are the subject. But users and providers of that data also have an interest and so should share responsibility for that stewardship. There is also a great need for public/private partnerships to cooperate in establishing new standards and open, yet secure, mechanisms for providing safe controls and a smoother user experience.

9. Reference

[AmericanBanker] – Penny Crossman, *Canadian Banks Manage Customers' Digital Personas; U.S. Banks Could Follow*, December 2013, http://www.americanbanker.com/issues/178_230/canandian-banks-manage-customers-digital-personas-us-banks-could-follow-1063980-1.html

[BurnerApp] - http://web.burnerapp.com/pages/press/

[Cate] – *Data Protection Principles for the 21st Century*, Cate et.al, March 2014, Oxford Internet Institute, http://www.oii.ox.ac.uk/publications/data_protection_principles_for_the_21st_century.pdf

[Eurocomms] - *Rob Chimsky, European Communications, 2013, "ARPA is Dead, Long Live ARPA".* http://www.eurocomms.com/features/opinion/9073-opinion-arpu-is-dead-long-live-arpa-

[GLBA] – *Gramm-Leach-Bliley Act*, U.S. Federal Trade Commission, Bureau of Consumer Protection, 2014. http://www.business.ftc.gov/privacy-and-security/gramm-leach-bliley-act

[GSMA[1]] - http://docbox.etsi.org/Workshop/2014/201405_PORVOO18CONFERENCE/SESSION_01_Introducing_Smart_Solutions/S01_Jutila_GSMA.pdf

[GSMA[2]] - ATKearney, *The Mobile Economy 2013*, p40, "Mobile Money for the Unbanked". http://www.gsmamobileeconomy.com/GSMA%20Mobile%20Economy%202013.pdf

[IDManagement]- http://www.idmanagement.gov/entities-cross-certified-federal-bridge

[ITU] - http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[McDonald] - Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society, 2008.* http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf

[NSTIC] – *"Three Pilot Projects Receive Grants to Improve Online Security and Privacy", Sept 2014,* http://www.nist.gov/itl/nstic-091714.cfm

[OASIS] - Oasis Electronic Identity Credential Trust Elevation Methods, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=trust-el

[OECD] – *OECD Work on Privacy*, 2013, http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines

[OIX] – http://openidentityexchange.org/resources/working-groups/telecom-data/

[Schneier] – Bruce Schneier, *Fingerprinting Burner Phones*, 2013, https://www.schneier.com/blog/archives/2013/10/fingerprinting_5.html

Other Recommended Reading

ARPU

http://www.fiercewireless.com/story/forget-net-adds-and-arpu-future-wireless-revenue-account/2012-05-21

http://www.cellular-news.com/story/Reports/36685.php

Informed Consent

http://techcrunch.com/2014/07/26/how-informed-consent-has-failed/