CYVA Research Corporation
Abstract

Data Slave Trade
An Argument for the Abolition of Digital Slavery: The Intrusive & Coercive Collection and Trafficking Of Personal Information for Profit and Power

---

For a Better Union of Social, Economic and Political Liberty, Justice and Prosperity Recognize and Secure the Mutual Rights & Responsibilities of Human-digital Existence

Contact:
Kevin O'Neil
Chairman & CEO
858 793 8100
koneil@cyva.com

Table of Contents

Document Audience, Structure and Purpose

This paper is directed to the general public, domestic and international. The paper is divided into three sections:

1) A description of the data slave trade and argument for recognizing human-digital existence. Within this section I retrace the historical practice of human slavery highlighting parallels to current abuses of our human-digital existence and the escalating de-humanization and exploitation of our digital identity for profit and power,

2) A path and strategy to pro-actively abolish data slavery and the status-quo that empowers the present industry and practice of personal information harvesting and exploitation. An actionable strategy of personal, community and legislative change is outlined,

3) A description of experimental inventions and services designed to empower individuals and communities to command and control their digital identities and information assets anywhere, anytime; to aggressively combat data slavery and assert our mutual rights and responsibilities of informational self-determination.

These proposed products and services are highly disruptive to present data brokerage and Internet advertising schemes that remain woefully hostile and toxic to citizen privacy and security. Competitive new user-controlled identity, Trusted Network Community and Trusted Information Utility products and services are outlined to restore trust in our digital economy, empower citizen-consumer human-digital rights and put individuals in charge of reaping the social and economic benefits of a trustworthy and secure digital identity.

There are three primary purposes or goals. One purpose is to educate the public, and position an instructive-catalyst metaphor that can be used to comprehend, relate to and provide a marshalling motivation for action in asserting human-digital rights and responsibilities. This educational process is designed to be interactive, collaborative and consensus building. It may serve as a basis for a Wiki or similar collaboration implementation.

Secondly, the paper is designed to act as a set of actionable tactics and strategies to guide and organize a forceful change in information politics. The battle over who controls and profits from the exploitation and manipulation of personal information is ever more present in the eyes of the public and rather take the position of being led as sheep to the slaughter it is time citizen-consumers took an informed inventory of their situation and began a just, values-based and constructive march toward restoring human dignity and liberty as human-digital beings.

Thirdly, there are emerging solutions to the issues raised in this paper and one set of inventions and services are being introduced with the intent to position them in a market of competitive inventions and potential solutions. It is hoped other products and services besides the author's can be presented through a future Wiki implementation of this paper and provide the public a view into the market of user-controlled identity and personal information management solutions.

Preface

Arguments concerning privacy and security are often conducted at the 40,000 foot level and although valuable at a principle level fail to reach pragmatically into the realm of our daily operational reality. The phrase 'boots on the ground' remind me of the bloody horrific reality of war and necessary dangerous and gritty entanglement that is necessary to root out a determined adversary. The ongoing debates and perplexities of privacy and security require such ground level, dirty detail entanglements with clear, unambiguous instruction for combatants in the field in ***how*** best to remain faithful to principle and yet find a sane and legitimate path to achieving a just and workable resolution amongst warring factions.

There is a war raging over who commands and controls personal information and who has legitimate authority to make us of, profit and/or benefit from such informational assets. This battle has been going on for years and has been escalating with each new clash of tech, governmental and corporate policy and practices that self-serving party's launch in pursuing organizational success, as they have defined it. All too often we citizen-consumers see and know a spiraling lose of control and dignity in our digital existence. The reality of growing harms perceived and real, is fearfully mounting.

As a citizen-consumer and peer amongst millions I wish to constructively voice a growing anxiety over the growing abuses and derelict powers that remain vocal but impotent in bringing a just and forceful new status, rightful power and mutual responsibility of human-digital existence. I believe there is a critical new awareness of our human-digital existence that is ready for empowerment.

Today we are struggling to understand and acknowledge the consequential realities of human-digital existence. There are observable cause and effect relationships between our digital and physical-psychological existence. Vulnerabilities in systems are being exploited with a raging identity-based crime outbreak mutating and spreading worldwide. Testified to by victimized millions laws and enforcement powers are weak and overwhelmed. So we are grasping painfully in brining principled law and order, while lobbyist, advocates and political powers negotiate competing interests that wage war every day in the embattled streets of cyber existence that traffic continuously and hazardously in human-digital material.

Slave Trade Metaphor

Metaphors can be powerful instruments in communicating and grasping an issue, acting as a catalyst for change. Metaphors have the power to shed new instructive light piercing and removing a fog of ambiguity and apathy that enables an uncomfortable stalemate. I wish to introduce and describe the ***data slave trade***, what it is and how we should use this characterization to reassess our values, beliefs and actions as they pertain to human-digital existence. There are consequences to characterizing issues that leverage particular metaphors and related human experience, our history as human beings. Metaphors have a tendency to marshal attention and bring a cognitively slippery and complex subject into a new relief that is painfully acute and real.

The concept of a data slave trade and what it means for and how it relates to our information society, our digital economy and how it may marshal political action is open

to possibility. We as citizens and corporate constituents and our law makers, I hope will consider such a metaphor in assessing what to do about privacy and human dignity in light of the fact (I argue) we are all being coerced daily into a new kind of slave relationship to masters who, for arguments sake have little regard for our well being and liberty or have at minimum decided for us that convenience, profits and so-called security are more important and must be given up and traded. Is this a Faustian bargain, a deceptive and dubious ploy?

My aim is to elevate a transformational idea. I wish to offer a constructive informed critique, outlining reasoned recommendations, hopefully leading to worthwhile change. I hope that this metaphor can spark and frame a reasoned and constructive dialogue leading to pragmatic solutions and actionable guidance. The slave trade comparison may be harsh with its supporting evidence but it is intended to marshal a well informed and motivated audience energized and ready to support reasoned solutions that go to the heart of this matter effectuating transformational change for the better.

If some do not like the term ***data slave trade*** and feel an uncomfortable conviction, so be it. I have seen far too much dysfunction and conflicted souls in organizations to want, in any shape or fashion, to enable an individual or organization in perpetuating a moral illness that harms self and others. I wish to inform and instruct and hopefully outline a path and means to addressing critical and often perplexing issues facing our information society and digital economy as we engage in our shared human-digital existence.

Network Community

I greatly value my network of friends and professional colleagues who provide a multidisciplinary perspective; a multidisciplined approach is critical. I am making this document available to those in my network community to deliberate, provide feedback, to further craft and optimize a multidimensional working framework of transformational concepts, political, business and architectural strategies that will support and empower needed changes in how we approach and apportion the power and sanctity of human-digital existence.

Each day we are contributing to and being influenced by an informational existence that is chaotically forming yet being skewed and manipulated in ways that obscures and denies our shared and mutual rights and responsibilities as human-digital beings, much of the manipulation for the sake of obscene profit and power. I hope this contribution, with the aid of many will constructively and forcefully contribute to a better human-digital world. I for one have been influenced much by an international community of data protection authorities, experts and advocates with much owed to the careful work of my own county's founders who sacrificially constructed the United States Declaration of Independence and Constitution, this is a primary inspiration and guide, and itself built upon the precepts of Natural Law.

1. Introduction: The Data Slave Trade

For centuries humans have enslaved other humans for profit and power. Empires have been built and sustained by the practice of slavery with persuasive economic and legal arguments made to justify the slave trade and its required de-humanizing attitude. The lure of wealth, opulent lifestyles and political power secured by the riches of slavery perpetuated and reinforced the business. However, in opposition, people were informed of the documented horrors and suffering of slaves, our human brothers and sisters, and began to march. With personal conviction many mobilized in mass, spoke out and marched towards abolishing slavery. Slavery as we knew it was outlawed[1], and nation by nation embraced the concept of fundamental human rights and liberties for all.

Figure 1: Slave being branded on the African coast.

Today there is a new kind of wealth creation built upon the backs of captives, our digital selves. As slaves of the transatlantic period were violently harvested from Africa, chained and branded, declared property of foreigners, we today have a new slave trader who with callous indifference harvest our personal information and puts it to work in very profitable advertising and marketing fields.

Exploiting personal information for profit is not new. However, this kind of commerce has reached an uncomfortable state of callous institutional empowerment and growing technological ubiquity that we all recognize with apathy ridden resignation, harboring growing fears and anger. Data surveillance technologies and practices created and espoused by darling search-engine wonders such as Google, Yahoo, and Microsoft, plus a collegial horde of data brokers and traffickers; your bank, the credit bureaus, our government are collectively building a staggeringly intrusive and pervasive means to capture, manipulate and exploit our digital lives.

Intrusive Internet technologies have been engineered with the express purpose of capturing, branding and putting to work our digital identities for profit and power. Billions are made each year in Internet advertising schemes with a crazed compulsion for more. More personal information, more richly cast digital profiles detailing our lives are being sold and resold, put to work in the data mines of big business without a dime being paid to the true and rightful owners and forget having any effectual control. So we today are like the African slaves, captured, branded, coerced, working but uncompensated, considered the rightful property of others that are making fortunes, perpetuating the trade.

"CEO Eric Schmidt admits that Google ads on mobile phones will be more than twice as profitable as Web ads because of hyper-personalization and targeting."

1.1. Our Human Dignity - What Dignity?

Today's callous traffickers, as their historical slave trader counterparts callously declare, "You have none, get over it." By force slave traders took hold of thousands denying their humanity, stripping them of any notion of free and equal, declaring them subhuman and mere property to be used as they saw fit. This was an exercise of power beyond right.

We, our digital selves are captive slaves and simply fuel for the economic engines of profit and power. And where is the law, protection of privacy, being secure and safe in our homes, our papers, our constitutional protections against unlawful search and seizure and involuntary servitude. We feel and know our informational self is being stolen each day in ways more pervasive and perplexing bundled with comforting promises of personalization, choice and security but the reality is quite the opposite. So, what are the law makers, the enforcement agencies and political powers doing?

1.2. Data Protection Laws: Unending Catch-up Game

A predictable response has been in play for 30+ years with data protection laws being promulgated world-wide but the laws have woefully lagged the trajectory of technology. Corporate lobbying over the years has effectively trumped the voices of citizenry and advocates with politicians compromising far too much in favor of big business interests. This is a race well suited to savvy corporate players who know well the game of political pacification and effective delay and dodge tactics. There are notable exceptions and growing omnibus legal coverage but laws take far too long to craft, decipher, deploy and remain considerably ineffective as technology and business practices run far ahead evading the well intentioned powers of authorities.

Yet today, as in the past, as the prolonged battle against slavery moved forward, there was and now is a new public awareness and readiness to confront and challenge what is becoming an alarming array of de-humanizing practices. The personal information collection and trafficking business is making us all slaves in a twisted economic malaise of greed and intrusive indifference to human dignity. Our data is simply out-of-control and available to far too many for harmful and demeaning exploitation.

1.3. Awakening: Informational Self-determination

There is an awakening occurring, a realization of the right of informational self-determination[2] – our individual and community rights and responsibilities to properly command and control personal information anywhere, anytime. This essential and fundamental right and liberty of informational self-determination is emerging, but embattled. We should be able to command and control our digital existence, our digital identity, our personal information, anytime, anywhere and should likewise respect others, our neighbors.

The right of informational self-determination is not an absolute. There are limits to informational self-determination within the bounds[3] of necessary individual and community imperatives that at times and under particular circumstances should override. However these human-digital rights and responsibilities should be fundamental, foundational and pervasively upheld and built-in as both legal and required operational infrastructure under girding our information society and digital economy rather than the ongoing mash-up of undermining technologies, practices and attitudes that perplex and anger us.

We are reminded of unlawful search and seizure protections and being safe in our homes and papers. Our personal papers, our intimacies, behaviors and inclinations are being explicitly targeted. Behavioral targeting is the rage as our Internet connected devices and appliances are used to turn our lives inside out for all who wish to plunder

and profit. Yes, there are benefits to personalization, but where is the “user-control” in such schemes? While we travel we are clad with parasite personal devices that silently surveil and steal our digital selves. Our life details, our habits, our location, our web browsing, our calls, our connections and interactions with others; the nitty details; this is the hyper-personalization and behavioral targeting information Google and others are aggressively securing. This personal information is a surreal treasure trove begging for assault.

1.4. Privacy and Human Dignity Taking a Back Seat to Profits and Power: Recognition and Resistance

Pervasive marketing is wholesale advertiser access to our once private and protected persona, our digital papers, the daily diaries of our lives is all being auctioned off for monstrous profits with privacy forced to take a back seat. Like Vegas, this entire game is rigged to profit the owners. And it really is convenient to communicate whenever, and connect to the Net and extend and enhance our lives as consumers. However, Rosa Parks recognized she was being wrongfully treated as second-class citizen and forced to sit in the back of the bus, to take a low demeaning position when other persons and prejudice prevailed. Our digital lives, our interests are being forced to take a back seat to commercial and governmental interests who argue they are forwarding our interests but we know this is nonsense.

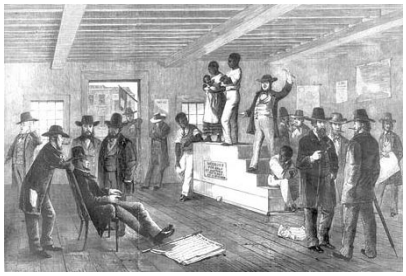


Figure 2: Slave Auction

We like Mrs. Parks recognize a fundamental failure in protecting human dignity. We are declared unworthy of a privileged and protected position. So often we are simply cargo to be shipped about a network of entities and processes seeking to manipulate and maximize profits and increase operating efficiencies. Slave ships packed themselves with horrific efficiency with little regard to human life. Of course you could not be too indifferent as this was a valuable cargo; there where acceptable risks and losses given oceanic travel.

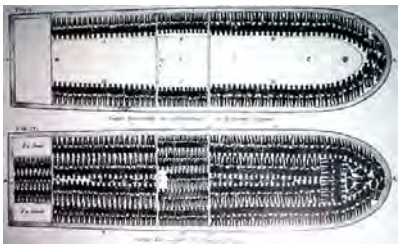


Figure 3: Slave Ship

Today databases are packed with raw human-digital cargo built with the understanding that the more you know about a person the more you can manipulate and maximize revenue. Being targeted for maximum consumerism is not without danger as security breaches and misuse of personal information is rampant. Identity theft today is taking a human toll; millions are exposed to cybercriminals who exploit the poor protections of human-digital material packed into systems that traffic continually in personal information. There is a wonton arrogant disregard for the wrongfulness unfettered data trafficking and mining at the expense of citizen privacy and security. An industry has flourished building and deploying identity

collection and processing infrastructures; a digital ecosystem that is wholly hostile and toxic to a free and self-determined digital existence is well underway.

With such effectual means to monitor and capture all things digitally me the fears of a police state with unparalleled powers of surveillance are not fiction, but a well understood and predictable result and modern reality. When federal agencies can bypass federal privacy laws and collect from commercial enterprise an unimpeded litany of personal information what barriers are left to secure a domestic population from such aggressive intrusiveness.

1.5. Appeal to the Past: Arguments for Human-Digital Dignity

"Am I not a woman and a sister?" Such questions and images sought to appeal to a society that benefited greatly by the existence of slavery, but many were now confronted by a moral appeal to abandon such practices and underlining beliefs in favor of a uncomfortable truth and necessity for change. We are experiencing the truth that a digital world does exist; we all have a digital existence; we are all digital beings and there are causal relationships between our digital existence and our physical and emotional existence. Real vulnerabilities and suffering occurs daily as millions are affected by data slavery. Changes and forces that occur within the digital world do affect our lives in the physical and psychological plane. As data moves and is altered to achieve the purposes of controllers they perform with near perfect calculation produce a desired change in physical, psychological, emotional, economic and political spheres.

Figure 4: Anti Slavery Petition

1.5.1. Use Case 1: Identity Theft

I exist as data. My data is stolen. It is used to create a false instance of my creditworthiness and used to make purchases in my name. I have just been violated and must now bear the burden of proving I did not perform this purchase of physical goods.

1.5.2. Use Case 2: A Painful Patient Record

I am a patient record. I am altered by another without my actual and verifiable consent. Poor authentication and access control now cascade and allow new bills and invoices in my name alleging I was a patient and medical expenses incurred and now I am responsible, but another person has benefited from my digital identity and cleverly impersonated me and received medical care in my name. Years go by and my digital records and self remain l infected and I continue suffering economically and psychologically by this past and ongoing abuse of my digital self. My creditworthiness reputation remains out of control and certainly out of my control.

1.5.3. Use Case 3: Job Seeker Vulnerability

I apply for a high security position and believe wholly in the necessity of a security background check but during the process my sensitive data: social security number, name, birth date, address is exposed haphazardly to 'trusted' insiders of whom all have

the capacity to snatch and sell my identity into a well orchestrated and profitable criminal enterprise. Insider breach is rampant with far too many trusted insiders empowered by institutional arrogance and willful negligence in providing unnecessary access fueling the profiting from and exploitation of my data.

1.5.4. Use Case 4: Road Warrior Encounters Information Warfare

I am pursuing the Web in search of a restaurant after a long international flight arriving at LAX. While mobile in person traversing the streets of LA, my digital self is being mashed-up in a traffic jam of digital brokers, buyers and sellers each honking and screeching for a profitable grab at my presence data: my location, my network ID, my behavioral profile all racked and stacked by algorithms in search of a perfect and very profitable vendor-ad-to-consumer-need transaction. So in search of a local restaurant my digital self is being Googled and groped by a so called trusted circle of paying participants; and I have some passing recollection of a privacy policy far to complex to navigate to bother to take the trip to fully understand so I clicked OK.

I am now ready to pick a sushi bar on Wilshire and don't have a clue that my ex-wife's divorce attorney is ready to pounce in caustic glee on this little but worthy bit of behavioral data; and yes my girl friend's location and our text message interactions are being mapped and analyzed by curious algorithms spitting out 'of interest' associations in the virtual back-office of the Sushi King on Wilshire. In tow, an orgy of state sponsored intelligence agencies (Russian, Chinese, U.S., British,…) intercept, store and analyze signal intelligence that is warehoused and cataloged as LAX traffic dated January 14, 2007. Corporate sponsored ease-dropping is scandalous when caught (e.g., HP) but goes on with carrier insiders being paid handsome bucks to track and listen in on whomever; and who else will be ready to steal and put my digital self to work in pursuit of knowing and using my digital identity far more than I care to imagine?

Fully mechanized information warriors intercept a blinding array of signal information, as the old saying in the intelligence business goes, "In God We Trust, Everyone Else We Monitor". As nation states compete for intelligence and counterintelligence prowess it is perhaps just a matter of time to see corporate road warriors and their employers commonly employ and afford sophisticated protective products and services for themselves to counter being compromised by state or corporate sponsored espionage activities and ambitions. What the DoD and intelligence agencies have in their arsenals of mobile devices and secure communications infrastructure is sure to be demanded and available given advances and lowering costs of such secure communications and surveillance counter measures.

1.5.5. Use Case 5: My 10-year Old Daughter Has Been Shanghaied

I and my wife are traveling today attending a wedding with our daughter safe with a sitter for the day. With social-networking boasting location services which are the rage amongst youth I am concerned but frankly unaware of the stealthy capture of my 10-year old daughters pictures, location patterns and customer proprietary network information (CPNI) data. She has been selected by a ring of professionals for a child sex slave industry that has proven adept and skilled in evading law enforcement; and is ruthlessly efficient. To my unbelieving horror my daughter has been included in a

catalog for high paying pedophiles awaiting shipment; an auction of sorts has fueled demand for her. Trusted insiders have provided timely location data used to signal a team that I and my wife are well out of range and evening's darkness has fallen.

My daughter's digital self has been set up for a fall into darkness. Taken as a digital captive she will be soon be employed without her parents knowledge, or assertive powers to prevent being kidnapped into a sickening world I thought was halfway across the planet and not lurking in an affluent neighborhood in California. Will present laws and promises from network operators prevent such a nightmare? My daughter will be stripped, gagged and bagged and made a precious meal for a monster.

I hope this technology (location-based services) can be used for good and not evil, but in the race for the fast buck safety and security have consistently been thrown to the back row a distant voice of sanity succumbed to the rage of the IPO and dazzling financial reward. Some firms have tarried and are responsibly taking time to faithfully consider the risk and make appropriate investments to better secure, command and control such sensitive data.

1.5.6. Use Case 6: The Escalating Viciousness of Media Fueled Voyeurism – The Paparazzi Pleasure Syndrome

The Paparazzi and their increasingly reckless and mean spirited assaults on celebrities is a graphic portrayal of an age old vice that is being systematically re-enforced and rewarded by an infectious print, cable and Net-based media. When actresses and actors fight back, seeking to somehow stay the intrusive onslaught of pernicious Paparazzi, we watch them twist in an agonizing futility that only seems to excite the masses for more. Watching Julia Roberts confront and scold her extreme and outrageous photo stalkers is news-entertainment but of the sort that enflames the question for many of us who would react the same furious way demanding why is there no law against this crap and why the hell are these assholes not in jail.

Julia like so many others is under siege by a horde of hunters that do not respect her choice for anonymity and liberty to choose her public-community in daily life. The argument is that she and others have NO expectation of privacy in a "public" space and its just life a 'concomitant of life in a civilized community' to be known by others. But what responsibility is there by us all to respect and protect the privacy wishes of any and all who would seek it, celebrity or not. What is characteristically a clash of freedom of the press interests and personal choice is being unequally charged by technology and a market that feeds upon the ability to instantly inform millions of the habits, whereabouts and persona of anyone.

"Exposure of the self to others in varying degree is a concomitant of life in a civilized community."- Brennan, J.[4]

"Freedoms of expression require 'breathing space.'" Rehnquist, C.J.

Yet our freedom is not license to do as we please but freedom to pursue virtue

Intentional provocation of citizen-celebrities and public figures is crass cruelty – the sort of taunting we see of caged animals done by mean spirited adolescents seeking to get a response to entertain themselves. For Julia Roberts and others such as Keanu

Reeves, Goldie Hawn, Jack Nicholson and numerous others there are calculated confrontations that are purposeful in seeking to get a reaction from celebrities, some going so far as aggressive heckling and badgering to incite retaliatory acts.

Exposure of the self in daily public life should not be subject to sadistic groping by cameras, our lives and persons being humped for profits by total strangers whenever and wherever we appear. Technology coupled with unfettered vice is nothing more than a weapon used to savage our privacy threatening and assaulting our right to be left alone – we all feel and know a need for human dignity and in our modern digital world we are seeing in the paparazzi a prelude to unfettered surveillance where our dignity as private people, or digital self-determination is stolen round the clock by others seeking to control and exploit our human-digital being.

NOTES: Diana Ross and The Supremes

Video http://www.youtube.com/watch?v=S_PKqgzSXAM

Stop! In The Name Of Love

(Brian Holland/Lamont Dozier/Edward Holland, Jr.)

Stop! In the name of love

Before you break my heart

Baby, baby

I'm aware of where you go

Each time you leave my door

I watch you walk down the street

Knowing your other love you'll meet

But this time before you run to her

Leaving me alone and hurt

(Think it over) After I've been good to you ?

(Think it over) After I've been sweet to you ?

Stop! In the name of love

Before you break my heart

Stop! In the name of love

Before you break my heart

Think it over

Think it over

NOTES:
Stop in the name of love. (Celebrity)
You have no rights to me.
But Baby, baby (Paparazzi)
I'm aware of where you go
Each time you leave your door
I watch you walk down the street
But this time before you run away
Leaving me alone and wanting more
(Think it over) After I've been good to you ?
(Think it over) After I've been sweet to you ?

I said stop in the name of love (Celebrity)
you have no rights to me.
So get along now…get along now."
No Baby, Baby (Celebrity Chorus)
You can't follow me
You have not rights to me
Now, I'm aware of where you go
Each time to cross the street
Me and my friends are ready to greet
But this time before you sneak a peek,
You'll need a license or face the judge
(Think it over) After they are done with you
(Think it over) Tossing and turning in your cell

So get along now…get along now.

You have no right to invade my space, to assault my dignity and put in harms way my life and those dear to me by your reckless and sadist pleasure in capturing a slice of my digital self.

Too much affirmative privacy here? To much to ask or expect given the fact celebrities make millions from well crafted and effectual public relations machines that intentionally seeks the public eye? Fact is we all guard our space and open and close the door to self as best we can. We invite others to join our time and space and unless we are acting upon some criminal intent is seems more than reasonable to give Julia and us all some 'breathing space' and demand proper notice, consent and under our terms the allowable capture and use of our digital identity and informational assets – informational self-determination.

1.5.7. Little Sister

I am your sister and I am a slave in a data slave market that routinely steals and sells my digital self, and I appeal to you to realize that this unrelenting drive towards the super profile and exploitation of all things digitally me is worthy of careful consideration and reflection on where this is heading and what kind of world we are creating. As past anti slavery activists appealed to our common humanity declaring masses of captive and chained woman our sisters, there is a parallel appeal to understanding and clarity of reason that challenges us to affirm the reality of a data slave trade. My little sister, my digital self does exists in a state of slavery and we are repeating in a dire new way the de-humanization of our humanity.

1.6. Natural Law Precepts as Applied to Human-digital Existence

If human-digital existence is to be affirmed, recognized and protected in kind as our natural human state as physical, psychological and metaphysical beings, what philosophical and moral framework should be employed and to what extent are past assertions of inalienable rights to be extended to our human-digital being? "John Locke argued that human beings in the state of nature are free and equal, yet insecure in their freedom. When they enter society they surrender only such rights as are necessary for their security and for the common good. Each individual retains fundamental prerogatives drawn from natural law relating to the integrity of person and property (natural rights). This natural rights theory provided a philosophical basis for both the American and French revolutions. Thomas Jefferson used the natural law theory to justify his trinity of "inalienable rights" which were stated in the United States Declaration of Independence."[5]

All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

-Article 1, Section 1 of the California Constitution

"…by the Fundamental Law of Nature, we are obligated to preserve not only ourselves but also other human beings – giving preference, in cases of conflict, to the innocent.

We would deny our common humanity with her in ignoring her cries for help just as surely as Old Man Wilkins denied it in taking her possessions by force.

1.6.1. Leveraging the U.S. Constitution and Natural Law Precepts

In Congress, July 4, 1776

The Unanimous Declaration of the Thirteen United States of America

….We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness. That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed, - That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness. Prudence, indeed, will dictate that Governments long established should not be changed for light and transient causes; and accordingly all experience hath shewn that mankind are more disposed to suffer, while evils are sufferable than to right themselves by abolishing the forms to which they are accustomed. But when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security.

4th Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particular describing the place to be searched, and the persons or things to be seized.

13th Amendment

Section 1. Neither slavery nor involuntary servitude, except as a punishment for crime whereof the party shall have been duly convicted, shall exist within the United States, or any place subject to their jurisdiction.

Section 2. Congress shall have power to enforce this article by appropriate legislation.

1.6.2. An Existence of Potential

In arguing for recognition of human-digital existence and an extension of Natural Law rights and responsibilities I argue that personal information has an innate potential. Personal information can be used for me or against me, to be employed to achieve a good or empower an evil inclination. It has potential for both. And once I seek to control the use of my human-digital existence don't I naturally have a right to purpose and direct this potential mindful of my responsibility to self and community of pursing good while avoiding evil.

Many different entities in our information society collect and process personal information and have views and policies that direct how personal information is used. Governmental, corporate, communities of all sorts, namely political action groups, your teachers union and more nefarious communities of terrorist and identity thieves form communities and use personal information just as all of us do as individuals.

Each of these collections use personal information for some purpose and conflicts of interest arise as whether that use is for or against us or our chosen community. The Department of Homeland Security/Transportation Security Administration collects airline passenger data and seeks to safeguard the traveling public. Terrorists attempt to infiltrate our transportation system and murder as many citizens as possible with the DHS/TSA pursuing various policies and practices in an attempt to prevent such acts. Conflicts of interest occur when citizen's object to police state like intrusiveness into our lives demanding in-depth identity verification and profiling; this we believe is a clear violation of constitutional privacy and forceful denial of our right to travel freely and anonymously without governmental or corporate sponsored "domestic surveillance".

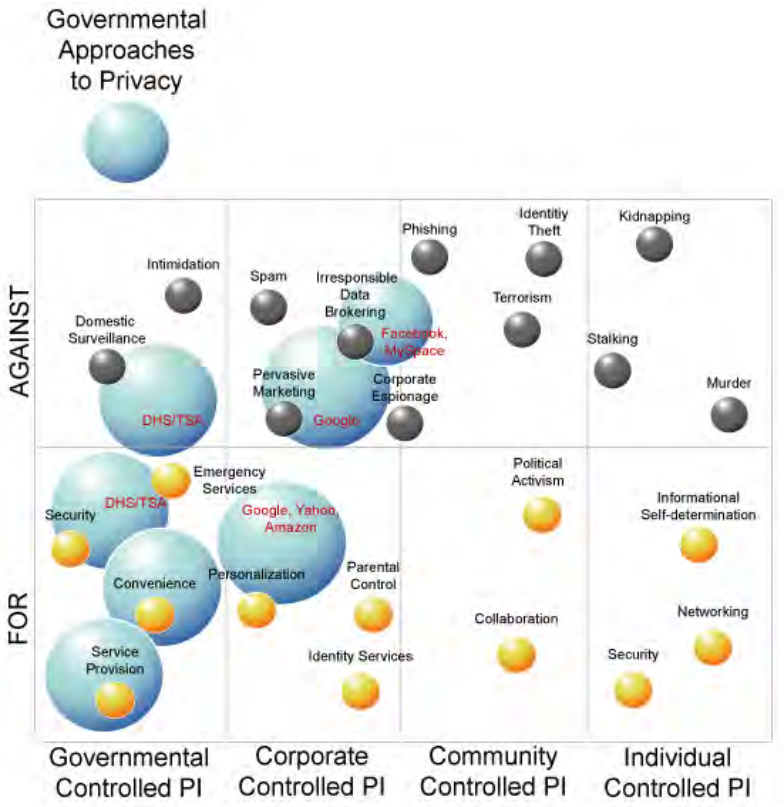


Figure 5: Information Used For and Against Ourselves

There are of course many reasons for citizen travelers to be very detailed about travel preferences and itineraries as we seek to plan, book and enjoy travel and hospitality services; and an identified personalization profile is essential. However, to what extent should law enforcement agencies have unfettered access to our identity, itineraries, arrangements and a cascading array of transactions that normally ensue during a trip? Is there a case for citizen-controlled trusted anonymous identity? Namely can I travel anonymously with minimal personal information available to TSA and airline agents perhaps just affirming my US citizenship (yes/no) and that is all. Call me passenger 24C, or a chosen pseudonym, Mr. Bob T (The Traveler). My ticket is a security token that is proof of purchase and enumerates the usual flight information but does not reveal anymore about me than I care to reveal.

In this scenario a Travel Identity Provider keeps a record of who exactly I am and affirms my trustworthiness as a airline traveler. Terrorist list will be maintained with identifiers that for now may mistakenly match a trustworthy traveler. It is problematic that crude identifiers such as a name can and do cause havoc with good people repeatedly being pulled aside for security searches.

1.6.3. The Good and the Bad of Data Brokering

Internet marketing schemes that rely upon the collection and processing of personal information and our "online" behavior has caused many citizen-consumers to cry foul. The out-of-control stealing of our digital lives at every click and turn of our online attention is putting us all in a paranoid and angry state of mind. It is troubling. Combine this with the aggressive data collection tactics of Facebook and other social-networking sites. Yes, my location is essential to fulfilling the convenience of getting real-time directs to wherever, but don't store this stuff beyond the needed few minutes this "take me to Sushi bar" process takes place.

my seat If I can explicitly infuse behavior namely my rules to my information that affirms and actualizes my will I, my human-digital self is now accountable for my choices as directed by my human-physical self.

My data is a reflection and image of my natural being, human-physical, mental and emotional being. Is this also a basis for extending human dignity to human-digital being? As a layperson to the realm of Natural Law theory and precepts argued over centuries I struggle to avoid science fiction and a debate of "digital life" and computer intelligence as another life form. That is not what I am leaning towards; but more pragmatically what beyond the my data as my property can be rationally and morally argued to correct a growing reality of virtual harms and abuses that pierce our physical-emotional reality.

My data is an image of me. I am created in the image of God. I have dignity and should recognize the dignity of all human creates as they are created in His image. My digital self is a reflection, in the image of my human-physical self therefore it to has the image of God and therefore deserves dignity.

Man's inhumanity to man has simply found another venue. A slave trade, past, now repeats itself in a new way. Free and equal under law needs to be extended to our human-digital existence. Claims to my personal information as the "property" of another based upon some exercise of labor fails to convince as we human beings are not naturally available to all for being deemed property of others; however, my labor is my own and I can use it to mix my labor with the common stock of natural things and now make them private property.

"John Locke observes that God has given the earth to man for his use and enjoyment. However, he seems to have given it to all mankind in common, for no one is born owning this piece or that. These two facts produce a paradox, because in order to use and enjoy something I have to withdraw it from the common stock; … when then can I appropriate things by mixing my labor with them? Only when they belong to the original common stock of nature."[6]

Laws that violate Natural Law are an act of violence

profiting and being coerced into

a certain and predictable loss of privacy and vulnerability to a new class of harms: identity-based crime and callous intrusiveness. What is coming to light is a characteristic truth of unfettered greed and unchecked totalitarianism: destruction of liberty and suffering masses.

Much of the wealth of Bristol was gained by exploiting African peoples, transporting them across the Atlantic Ocean in horrific conditions, and selling them into slavery in the new world.

In addition significant numbers of African people were brought to Britain from the West Indies (a voyage of double horror) to be sold in Bristol (although this was against English law) and forced into service in merchant's and aristocrat's households.

Slave being branded on the African coast. Artist unknown WPA Book 1940

1.7. Backlash: A New Public Force for Change

There is a new fear in corporate echelons. The media driven exposure of corporate and governmental data breaches and barrage of identity theft coverage and reality of a hostile and toxic digital ecosystem has placed the argument for change on a new plane of possibilities. With 40+ million identity theft victims to date in the U.S. with bio-weapon efficiency a staggering rate of 10-15 million victims are being added to the rolls. This is out of control and escalating world-wide, there is now an army of more than willing citizen-consumer soldiers ready to march for a new status-quo in the game of who commands and controls personal information.

1.8. Pay Me or Release Me: I am Not Your Property

Involuntary servitude: “Involuntary servitude is a United States legal and constitutional term for a person laboring against that person's will to benefit another, under some form of coercion. While laboring to benefit another occurs in the condition of slavery, involuntary servitude does not necessarily connote the complete lack of freedom experienced in chattel slavery; involuntary servitude may also refer to other forms of unfree labor. Involuntary servitude is not dependent upon compensation or its amount.

The Thirteenth Amendment to the United States Constitution makes involuntary servitude illegal under any US jurisdiction whether at the hands of the US government or in the private sphere, except as punishment for a crime: "Neither slavery nor involuntary servitude, except as a punishment for crime whereof the party shall have been duly convicted, shall exist within the United States, or any place subject to their jurisdiction." According to lectlaw.com[1], involuntary servitude is defined as servitude to a person, which excludes the US government and its political subdivisions.”

made to be chattel of other men, nor enslaved for life

Sugar growing is a labour-intensive undertaking and Portuguese settlers were difficult to attract due to the heat, lack of infrastructure, and hard life. To cultivate the sugar the Portuguese turned to large numbers of African slaves. Elmina Castle on the Gold Coast, originally built by African labor for the Portuguese in 1482 to control the gold trade, became an important depot for slaves that were to be transported to the New World.[43]

1.9. When Business is Good it Spreads Like a Disease

Increasing penetration into the Americas by the Portuguese created more demand for labour in Brazil--primarily for farming and mining. To meet this demand, a trans-Atlantic slave trade soon developed. Slave-based economies quickly spread to the Caribbean and the southern portion of what is today the United States. These areas all developed an insatiable demand for slaves. As European nations grew more powerful, especially Portugal, Spain, France and England, they began vying for control of the African slave trade, with little effect on the local African and Arab trading. Great Britain's existing colonies in the Lesser Antilles and their effective naval control of the Mid Atlantic forced other countries to abandon their enterprises due to inefficiency in cost. The English crown provided a charter giving the Royal African Company monopoly over the African slave routes until 1712.[44]

http://en.wikipedia.org/wiki/Atlantic_slave_trade

http://en.wikipedia.org/wiki/Atlantic_slave_trade

At the 2001 World Conference Against Racism in Durban South Africa, African nations demanded a clear apology for the slavery from the former slave-trading countries. Some EU nations were ready to express an apology, but the opposition, mainly from the United Kingdom, Spain, Netherlands, Portugal, and the United States blocked attempts to do so. A fear of monetary compensation was one of the reasons for the opposition. Apologies on behalf of African nations, for their role in trading their countrymen into slavery, also remains an open issue.

Are you blind or just in denial of the fact you are a slave trader and just as reprobate as your historical predecessor.

I should be able to control the use of my data and once exchanged remain in control throughout the life of the data; this is my life, my digital existence and persona.

1.10. Born into Data Slavery: How respected Intuitions such as Healthcare go along and get along with the data slave trade

On January 30, 2006, Jacques Chirac said that 10 May would henceforth be a national day of remembrance for the victims of slavery in France, marking the day in 2001 when France passed a law recognizing slavery as a crime against humanity.[61] When will it be acknowledged and confessed that while mothers prepare to give birth back office deals have been sealed transfer birth records and so called protected heath records on to data brokers who make a fast buck while baby kicks in the womb; and before mom get home she and child are welcomed by an onslaught of magazines and pitches for material stuff. Yes, some of this stuff might be useful but the price to human-digital dignity and informational self-determination far too great.

“The day you were born your digital self was sold into slavery never to see the light of self-determination”

Now the newborn in our physical world is now mirrored by an aborted digital brother or sister that now sits captive in a data factory who’s only intent is to work this data sibling

as long as it lives for producing more profits and power to its new owner. The day you were born your digital self was sold into slavery never to see the light of self-determination: the freedom to choose and be one with human self. Our digital lives are begun all too often as stolen children sold immediately into a non-consensual labor force, what should be recognized as slavery with national leaders fully believing and pronouncing this crime against humanity as we are human-digital beings and should be recognized as such, empowered and protected by inalienable rights.

1.11. Maternal Instinct & Social-networking: Don't Mess with Mother Bear

With the raging popularity of social-networking sites such as Facebook and MySpace there has emerged a reactionary and resolute force of concerned parents who ask a simple question: "Is this safe for my child?" When faced with the facts of documented pedophile seductions, identity-based crime, state AG prosecution of 20 something males pretending to be adolescent boys who lure and rape young 14 and 15 year-old girls, and victim lawsuits and episodes being broadcast by the media, parents instinctually pull the plug. And some pulling the trigger on a double barreled shotgun of 'not over my dead body' criticism.

Women, the mothers have a special visceral rage reserved for those who represent a clear and present danger to their young. Mothers instinctually will marshal untapped reserves of energy and purpose taking on any who, no matter how powerful, threaten their children. But why has social-networking management so stubbornly evaded and resisted meaningful and effectual safeguards demanded by state AGs and parents; and is funding well orchestrated public relations campaigns buying the 'trusted' opinions of Internet safety advocates to counter the harmful documented realities?

Answer: eyeball-driven Internet advertising schemes rely heavily on traffic. Any encumbrance to site traffic is viewed as detrimental to advertising profit and so the protections sought by parents and AGs is viewed as a threat to revenue. The phenomenon of millions freely sharing and perusing their digital identity, uploading billions of bits of user-generated content has spawned a huge cache of potential ad revenue, however the evidentiary facts mount with a clear abhorrent trail of abuse and 'digital identity' vulnerabilities that plague social-networking sites that manifest a careless and cruel disregard for human-digital existence.

With legislation being crafted and proposed by states and federal efforts underway it appears inevitable that some form of identity controls will be crafted that seek to create a safe and secure space for children or adults to be digital and enjoy the ability to socialize and participate in online communities.

2. A Proposed Path for Change: Personal Political Action

The intrusive and coercive collection and trafficking of personal information is escalating. Many continue to suffer the onslaught of in-your-face hostility to "leave me alone" resistance. There is Paparazzi attitude and drive that coldly and callously reasons that it is okay to steal and abuse our human-digital dignity anytime they want and no one can stop them. Existing privacy laws and regulations have struggled to reach effectively into this abyss of growing abuses. To the hardened Paparazzi crew, including all who steal and swipe our digital lives, the laws are to be ignored, cleverly

worked around and evaded, as they know it is simply to expensive and difficult to enforce; catch me if you can. This will and must change.

One way, one path is to marshal personal political action that flows from the community, peer to peer and spreads virally. Articulating, educating and equipping others with a set of human-digital rights and responsibilities that are self enforcing; they represent a set of personal values and beliefs to be adopted internally and effectuated in our daily interactions with our family, friends and neighbors who like us are fed up with the status-quo. This will transform and vitalize a community that will then deal with the institutions.

2.1. On the Legislative Front: Recommendations for Collaborative Consideration

Below is a list of acknowledgments and recommendations that are being offered for collaborative consideration. It is hoped these can used as a basis for discussion and debate in forming a set of values, laws and regulations to advance a society and economy better able to pursue justice, liberty and mutual respect and allegiance to defend and protect one another.

California Human-digital Rights & Responsibilities Act

1. Recognize human-digital existence and empower a comprehensive, coherent and enforceable protection of human-digital dignity as a free and equal being with certain enumerated rights and responsibilities.
2. Recognize that information society and a digital economy is dependent upon a secure, fair and equitable sharing and processing of human-digital identity and that protections and affirmations of human-digital dignity are necessary protecting our security and liberty.
3. Recognize that information society is becoming more a surveillance society with an ever escalating and ubiquitous capacity to detect, trace and track citizen identity and behavior. There is an urgency to re-enforce and re-assert citizen privacy and informational self-determination rights and systematically curtail this trend towards a surveillance society. The commercial pursuit of super-profiles and providing such data to governmental agencies is also increasing, with agencies seeking to circumvent federal (U.S.) privacy protections. This too should be better controlled with citizen assertive means to prevent and more effectively control (turn on, turn off, throttle) such collection and trafficking.
4. Recognize that it is necessary to authoritatively and assertively protect human-digital dignity and that related personal information has an intrinsic personal, social and economic value. Personal information as a societal resource should be comprehensively protected, recognizing we are creating and participating in a global digital ecosystem that is interconnected and dependent. Ongoing failures to secure human-digital rights and enforce necessary responsibilities across geo-political and jurisdictional boundaries is enabling widespread criminal behavior and a catch-me-if-you-can mentality of exploitation and irresponsibility.
5. Recognize the value of comprehensive, coherent and actionable legal precepts such as fair information practices are critical to guide and state privacy principles but require operational frameworks to better guide and maintain ‘true to the spirit

of the law' compliance by custodians and users of human-digital identity and related information assets.

6. Recognize that a flexible and manageable taxonomy of human-digital data detailing the type, format and semantics of human-digital identity and related information assets is vital to administrating a well managed information society and economy.
7. Recognize a distributed meta data dictionary that can be used to administrate and map differing taxonomies, elements or system artifacts can benefit individuals, communities and controller entities in advancing interoperability and secure exchange and reliable processing of human-digital identity and information assets.
8. Recognize that a secure, robust, reliable, manageable and human understandable human-digital (privacy) rights and responsibilities language is necessary for just and secure citizen-controlled digital existence that with preserve a values-based information society and economy.
9. Recognize that innovation is necessary to improving and accelerating advances in human-digital existence and application of Natural Law precepts for a better information society and economy.
10. Recognize free choice and information self-determination must be guided and bounded by Natural Law and the obligation of all to protect and defend one another is essential
11. Recognize that conflicts of interests in the proper use and obligations of human-digital existence and related identity and information assets will arise and detailed use cases specifying actors, objects, data flows, motivations and particular operational uses of identity and information assets need to be fully documented and made available to vested parties to examine and voice judgments.
12. Recognize that inventions that collect, store, process and exchange are susceptible to risks that may impact citizens or their community and that it is prudent to test, verify and disclose vulnerabilities and standardized protection profiles to inform the public of a device, system or enterprise capacity to protect and assert citizen's right of informational self-determination. Low, medium and high security and privacy assurance labeling of products and services should be mandatory with clear documentation of specific personal information elements processed by the device or service.
13. Recognize that trustworthy information utilities and network communities can be constructed and operated to secure and enforce human-digital values and such entities are free to operate as regulated or self-regulated entities with the public's free will to join, participate in, and govern such utilities and communities.
14. Recognize the need for an authoritative and independent information utility commission (IUC) made up of a multidisciplinary (legal, audit, IT security,

information system architect or engineer, business, privacy advocate, and citizen) body of representatives to hear and adjudicate privacy complaints (private actions and class actions brought by agents of the court under contract and license to avoid self-enrichment and corruption by attorneys or parties seeking unfair remedies). The IUC shall be responsible for maintaining legal and operational standards for the protection and assertion of privacy and informational self-determination rights and responsibilities. The commissioners shall serve staggered 4 year terms rotating 1/3 of the 9 member commission. Seven members comprise the commission's multidisciplinary representative with each category represented by one qualified individual with a secondary alternate representative. All qualified commissioners are nominated by the people in a popular vote with campaign resources made available to candidates. Two members are to be qualified data protection authorities acting as the IUC Chief Commissioner and assistant commissioner. The Chief and Assistant Commissioners are nominated and elected by the people of the state of California every 4 years.

[comment: need further research on means to thwart insurmountable financial resources and contributions in influencing a vote. Campaign reform laws still evolving and effective means to curtail efforts by powerful organizations in "buying" seats on the IUC. One thought was to have a random selection of top 10 candidates to dampen efforts to skew an election process and provide all candidates a online means to present themselves and respond to questions from voters.]

15. Recognize that there are benefits to an information society and economy that individuals have a right to freely engage and abide by personal information rights and responsibility agreements or contracts with other individuals or organizations to share in the values-based use of digital identity and information assets; and that model contracts and a informational rights and responsibilities language that can be bound to digital identity and information assets is worth advancing.

16. Recognize that we all are exposed to uninvited intrusions into our private lives by celebrity journalist "Paparazzi" and that the unfettered collection of human-digital identity is a violation of informational self-determination. Those who profit from the collection and exploitation of photographs, videos, sound recordings of persons of interests should be regulated. Licensing and regulation of celebrity journalist is necessary to protect the citizen's right of informational privacy and pre-emptive protection from extreme and outrageous conduct that continues to escalate. It is recognized that out-of-control Paparazzi practices continue to effectively fuel a crazed compulsion for more inflammatory and dangerous acts that put at risk the lives of citizens. Effective regulation is now needed.

    a. Licensing of Celebrity Journalist is mandatory.

    b. Citizens who wish to maximize human-digital rights protection should register with their Community Review Board. Any citizen seeking such protection will not be refused registration. Citizen's need not be celebrities or public figures.

c. C-Journalist must be visually distinguishable by a uniform or jacket with insignia.

d. C-Journalist must be detectable by secure wireless ‘presence’ devices with built-in GPS that provide citizens a means to detect and examine C-Journalist credentials.

e. C-Journalist can only use licensed human-digital rights (HdR) enabled equipment (cameras and video recorders) to capture images and other recordings with autotagging that at minimum include: geotagging capabilities, facial recognition to prevent or allow registered citizens from illegal photo or video capture, secure date/time stamping, C-Journalist identification and binding HdR rules.

f. C-Journalist cannot capture human-digital identity or information assets without the consent of citizen-subjects.

g. C-Journalist shall register and schedule with Agents representing clients or the citizen-clients themselves for photo shoots, interviews or HdR recordings.

h. C-Journalist authorized activities while underway can be stopped immediately upon command by citizen-subjects or their agents.

i. If C-Journalist fail to obey cease and desist orders from citizen-subjects or their agents the use of non-lethal force are allowed. Citizen-subject must be allowed to defend themselves against unrelenting assaults

j. Citizen-subjects or their agents will be provided licensed secure signaling devices that empower targeted, unilateral disablement of HdR recording equipment. C-Journalist can override such shut-off with a one-time key but must claim an exception. The HdR device will signal authorities of either a Citizen-subject triggering or C-Journalist use of an override. Such exceptions will be investigated and adjudicated by Community Review Boards.

k. All C-Journalist recordings are subject to review by citizen-subjects or their Agents who have the sole authority to set information utility rights for any HdR recordings.

l. Community Review Boards and local enforcement officers (police) will be available 24/7 to receive complaints by citizens of unauthorized capture and exploitation of personal information (unlawful use of HdR recordings), physical assault, reckless endangerment, stalking, harassment, intimidation, taunting or other psychological harms.

m. Community Review Boards shall maintain public C-Journalist profiles that contain ‘reputation’ ratings and history of both positive and negative remarks by Authorities, citizens and Agents.

n. C-Journalist shall have the right to comment on any ‘reputation’ records and histories.

o. C-Journalist public records can be purged provided fines, and penalties are paid in full and erasure of such public records must have the consent of incident victims and or their Agents.

p. Punishment for C-Journalist crimes and others acting as unlicensed C-Journalist shall include loss of C-Journalist privileges, monetary fines, and mandatory jail time.

q. Proportional punishments are due any collaborative entities or other persons that traffic in any unlawful human-digital identity or information assets.

r. C-Journalist’s abilities to capture images, recordings, and other HdR records shall not be restricted when it falls under an exception rule.

s. Exception rules include protection of the citizen-subject or others, documenting illegal acts by citizen-subjects, authorization to capture HdR recordings by judicial authorities in accordance with constitutional due process, or a clear and present ‘sanctity of life’ interest.

t. Funding for the C-Journalist licensing program, Community Review Board staffing, operations, and enforcement officers should be derived from a 7.5% information asset utility fee. C-Journalist will pay an annual license fee not to exceed X and be bonded.

17. Recognize the regulatory value in model contracts (corporate binding rules) that provide unified coverage for custodians and users of human-digital identity and information assets across jurisdictions and geo-political boundaries.

18. Recognize security must empower individuals and organizations to achieve their goals and objectives and not unnecessarily impede or circumvent, but protect a prudent course and capability of action. There is a classic tension we as security professional must address daily as we seek to optimize individual and organizational performance and faithfully protect and affirm our constitutional values as free and equal citizens in a world of serious threats and intentions to destroy these ideals.

2.2. California Human-digital Rights & Responsibilities Act

For a better union of social, economic and political liberty, justice and prosperity recognize and secure the mutual rights and responsibilities of human-digital existence.

It is imperative that new formative laws be put into place to comprehensively secure, protect and conserve human-digital dignity, our digital identity and related personal information assets. These laws should affirm the inalienable right of informational self-

determination – our information privacy and the affirmative right to command and control our personal information anywhere, anytime and according to citizen terms, rules and directives derive value or benefit from the secure and trusted use of their personal information assets.

Our digital economy and information society is being undermined by the reckless and wonton profiteering and exploitation of personal information. Unrelenting ambitions for profit and manipulative powers at the expense of human dignity and constitutionally protected liberties have and continue to exploit personal information with dire and documented results now prevalent in our society.

Specific and effectual laws and regulation are needed to recognize and affirm human-digital being and that we as humans do exist as informational entities that are not only created in our image but represent a protected type of existence with enumerated rights and responsibilities. It is affirmed that the right of informational self-determination is not an absolute right that prevails in all contexts and circumstances, but must yield at times and in particular situations to a set or mutually held individual and community responsibilities.

At times it is necessary to be fully transparent in our digital being, fully identifiable, and have data processing actions performed that satisfy a necessary set of rules of interaction and social intercourse without such controls unnecessarily puts at risk relying parties who seek to affirm both our good will and our liberties e.g., liberties in free and unobserved travel. Example: A trusted anonymous travel identity wherein credentialed anonymous travelers can affirm a level and type of identity for boarding flights but not unnecessarily reveal identity attributes to persons or systems that do not have a need to know but simply affirm a level of trustworthiness as vetted and credentialed by travel authorities and/or identity authorities.

2.2.1. Promulgated Laws Must be Understandable & Enforceable

“Thomas Aquinas says that if a law is not promulgated it is not really a law at all…a law that the people cannot understand is like a law that has never been promulgated.”

NOTES “There is a fairly broad and international consensus on the principles, often termed “fair information practices,” that ethically (and often legally) must be taken into account in handling information about individuals. These include the notion that personal data should be collected and processed for defined and legitimate purposes, with fair notice to the individual, mechanisms for exercising choice (consent) wherever the individual’s privacy interests outweigh competing public or private interests, opportunities for access and correction by the individual, an appropriate level of information security, and practical methods of enforcement and recourse in the case of abuse or negligence.

But these principles of fair information practices are implemented differently, often with substantial variations in terminology, legal requirements, and technical and operational mechanisms, from country to country, sector to sector, and application to application. Privacy principles are a necessary foundation, but something more is required to achieve consistent, compliant, interoperable privacy and security solutions throughout an organization and across sectoral, state, or national borders.”

It is recognized by the data protection community[7] that "privacy by design" namely the engineering of privacy principles into technology-based products and services must be advanced.

2.2.2. Translating Law into Operational Infrastructure

"One of the tasks that ISTPA has set for itself now is to map some of the more important privacy legal regimes to the Framework, showing how it can be used for compliance purposes. Another is to show how the Framework services can be automated in some particular use cases. Our hope is that this will pave the way for practices that will work across a global company, for example, or the development of software solutions that can be applied to track and protect personal data across applications and users. The Framework can serve as a "requirements middleware" that bridges the differences in terminology and scope from one privacy regime to another and provides a standardized operational translation of legal requirements to operational requirements simplifying compliance with applicable laws, promises, and internal policies.

The Framework will not, of course, end the debate over appropriate policy choices that affect privacy. The privacy services defined in the Framework are themselves "policy-configurable" in each case. The Framework and underlining use case approach in gathering requirements can be used to facilitate the identification of options and solutions in each case; it provides a common vocabulary and toolkit empowering a more robust and definitive means in capturing and communicating privacy policy complexities, their context particulars and related issues. It is expected that a Framework-based use case repository and toolkit will greatly aid practitioners in designing and implementing operational solutions."

The right of informational self-determination, the right to command and control our personal information should be explicit and enumerated as a set of information operations and behaviors that can be captured in human readable, understandable, unambiguous and as needed granular means. A human-digital rights and responsibilities expression language is needed to capture rules and preferences of informational being operations and behavior that can be communicated, enforced and audited.

Operations could include: create, read, update, delete, view (display before human operator), execute or play (video or audio file), store, archive, encrypt, decrypt, join, compare, transform, label or classify as, export, exchange for, transfer. Such a language would help clarify understandings between data controllers, custodians, processors and human-digital beings and their human counterparts.

2.2.3. Privacy Requirements: Composite Operational Definitions

The International Security, Trust and Privacy Alliance[8] has labored to comprehensively review current privacy legal and regulatory instruments to develop a "harmonized" terminology that would capture the core meaning and intent of each legal instrument

and principle. The ISTPA's analysis resulted in the following operationally-focused working definitions.

Following are the ISTPA's "Composite Operational Definitions":

1. **Accountability:** Reporting made by the business process and technical systems which implement privacy policies to the individual or entity accountable for ensuring compliance with those policies, with optional linkages to sanctions.
2. **Notice:** Information regarding an entity's privacy policies and practices including: definition of the personal information collected; its use (purpose specification); its disclosure to parties within or external to the entity; practices associated with the maintenance and protection of the information; options available to the data subject regarding the collector's privacy practices; changes made to policies or practices; and information provided to data subject at designated times and under designated circumstances.
3. **Consent:** The capability, including support for Sensitive Information, Informed Consent, Change of Use Consent, and Consequences of Consent Denial, provided to data subjects to allow the collection and/or specific uses of some or all of their personal data either through an affirmative process (opt-in) or implied (not choosing to opt-out when this option is provided).
4. **Collection Limitation:** Constraints exercised by the data collector and user to limit the information collected to the minimum necessary to achieve a stated purpose and when required demonstrably collected by fair and lawful means.
5. **Use Limitation:** Controls exercised by the data collector or data user to ensure that personal information will not be used for purposes other than those specified and accepted by the data subject or provided by law, and not maintained longer than necessary for the stated purposes.
6. **Disclosure:** The release, transfer, provision of access to, use for new purposes, or divulging in any other manner, of information by the entity holding the information only with notice and consent of the data subject; the data collectors policies must be made known to and observed by third parties receiving the information, and sensitive health information disclosures must be managed.
7. **Access and Correction:** Capability allowing individuals having adequate proof of identity to find out from an entity, or find out and/or to correct, their personal information, at reasonable cost, within reasonable time constraints, and with notice of denial of access and options for challenging denial.
8. **Security/Safeguards:** Policies, practices and controls that ensure the confidentiality, availability and integrity of personal information collected, used, maintained, and destroyed; and ensure that personal information will be destroyed or de-identified as required.
9. **Data Quality:** Ensures that information collected and used is adequate for purpose, relevant for purpose, not excessive in relation to the purposes for which

it is collected and/or further processed, accurate at time of use, and, where necessary, kept up to date, rectified or destroyed.

10. **Enforcement:** Mechanisms to ensure compliance with privacy policies, agreements and legal requirements and to give data subjects a means of filing complaints of compliance violations and having them addressed, including recourse for violations of law, agreements and policies.
11. **Openness:** Availability to individuals of the data collector's or data user's policies and practices relating to their management of personal information and for establishing the existence of, nature and purpose of use of personal information held about them..
12. **Anonymity:** A state in which information or data are rendered anonymous so that the data subject is no longer identifiable.
13. **Data Flow:** The communication of personal data across geo-political jurisdictions by private or public entities involved in governmental, economic or social activities.
14. **Sensitivity:** Specified data or information, as defined by law, regulation or policy, which requires specific security controls or special processing.

2.2.4. ISTPA Privacy "Operational" Framework

There is clear need for operational standards to advance privacy and security.

NOTES from ISTPA Privacy Framework

The Framework will not, of course, end the debate over appropriate policy choices that affect privacy. The privacy services defined in the Framework are themselves "policy-configurable" in each case. The Framework and underlining use case approach in gathering requirements can be used to facilitate the identification of options and solutions in each case; it provides a common vocabulary and toolkit empowering a more robust and definitive means in capturing and communicating privacy policy complexities, their context particulars and related issues. It is expected that a Framework-based use case repository and toolkit will greatly aid practitioners in designing and implementing operational solutions."

Service	Description
Audit	Handles the recording and maintenance of events in any service to capture the data that is necessary to ensure compliance with the terms and policies of an agreement and any applicable regulations.
Certification	Manages and validates the credentials of any party or process involved in processing of a PI transaction.
Control	Functions as "repository gatekeeper" to ensure that access to PI which is stored by a data collection entity complies with the terms and policies of an agreement and any applicable regulations.
Enforcement	Handles redress when a data collection entity is not in conformance with the terms

	and policies of an agreement and any applicable regulations.
Interaction	Presents proposed agreements from a data collection entity to the data subject; receives the subject's personal information, preferences, and actions; confirms actions; manages movement of data into and out of the Framework. To the extent the data subject is represented by an agent, this service comprises the interface to the agent.
Negotiation	Handles arbitration of a proposal between a data collection entity and a data subject. Successful negotiation results in an agreement. Humans, agents, or any combination, can handle negotiation.
Validation	Checks for accuracy of PI at any point in its life cycle.
Access	A service that allows the data subject to both access the individual's PI that is held by a data collection entity, and to correct or update it as necessary.
Agent	A software service that acts on behalf of a data subject or a requestor. The Agent Service engages with one or more of the other services defined in this Framework. Agent can also refer to the human data subject in the case of a manual process.
Usage	Functions as "processing monitor" to ensure that active use of PI complies with the terms and policies of an agreement and any applicable regulations. Such uses may include transfer, derivation, aggregation, pseudo-anonymization, linking, and inference of data.

2.2.5. Bodily integrity and integration

It is critical to recognize the actual and potential harms done when an individual's personal information is stolen and fraudulently used. When a living human body is pierced we say that that their bodily integrity has be violated. Human-digital beings as parts of our oneness are separated violently from us by force or coercion represent a violation of bodily integrity. Such separations should be remedied and brought back to a state of original and viable human-digital command and control. If I cannot freely communicate with nor command and control without coercion my digital self I am in a state of disintegration and separation.

2.2.6. Secure in their persons

My human-digital self should not be captive and held under a full, partial informed or a secret state. Unless my human self is in a state of protected due process My human-digital self

2.2.7. Digital Persona Ontology

The right of informational self-determination, the right to command and control our personal information should be explicit and enumerated as a set of information operations and behaviors that can be captured in human readable, understandable, unambiguous and as needed granular means. A human-digital rights and responsibilities expression language is needed to capture rules and preferences of informational being operations and behavior that can be communicated, enforced and audited.

Operations could include: create, read, update, delete, view (display before human operator), execute or play (video or audio file), store, archive, encrypt, decrypt, join, compare, transform, label or classify as, export, exchange for, transfer. Such a

language would help clarify understandings between data controllers, custodians, processors and human-digital beings and their human counterparts.

2.2.8. Privacy Rights Expression Language

NOTES

Taxonomy and privacy rights expression language

Subject to <conditions> and <security> requirements,

allow <action> for <purpose>,

where data is <category> about <identity>,

from <source> to <recipients>,

with <obligations> and <retention requirements>.

2.2.9. Trust No One: The Necessity for Verifiable Accountability

“Trust no one” is a policy everyone should heed with regards to safeguarding their personal information. What follows is a pragmatic criteria and mantra for all those who wish to responsibly protect themselves and those within their network community: Trust No One, Especially Those Who Refuse Accountability. And when a party wishes to affirm accountability, that accountability must be verifiable by independent, impartial and thorough inspection accompanied by effective enforcement powers (technical and legal) to halt illegal collection and processing of personal information.

What the PI governing rules are will be significantly enhanced by an unambiguous and PI-specific privacy rights and responsibilities expression language. It is up to individuals, their fellow citizens, authorities and usage community to agree on the specifics given a particular context and circumstances that are guided by higher principles such as the human-digital right of dignity and informational self-determination. Again, such a principle should not be taken as an absolute as there are necessary exceptions wherein the type of identity being processed will take different forms taking into account an optimal mixture of constraints and controls needed to safeguard human-digital identity and information assets.

Who guards the guardians is and will remain a classic issue facing our information society as we collectively seek to maximize the benefits of human-digital existence and a just and equitable use and conservation of personal information assets. The establishment of Trusted Information Utilities and a framework for the establishment and operation of such entities is proposed.

Security must empower individuals and organizations to achieve their goals and objectives and not unnecessarily impede or circumvent, but protect a prudent course and capability of action. There is a classic tension we as security professional must address daily as we seek to optimize individual and organizational performance and faithfully protect and affirm our constitutional values as free and equal citizens in a world of serious threats and intentions to destroy these ideals.

2.3. California Information Utility Act: Protecting and Conserving Our Shared Digital Assets

To restore trust in our digital economy and set a foundation for a just and equitable information society and culture that recognizes, affirms and aggressively empowers the human-digital being and the rights of citizens to responsibly command and control their digital existence. To affirm and empower these rights and responsibilities a body of statutory protections, administrative oversight and guidance, grants for research and development and the formation of *information utilities* that govern and protect personal information are recommended.

There is a growing need for organizations (private and public, for-profit and non-profit) to lesson the burden of regulatory complexities and conflicts with regard to privacy laws world-wide. Standardizing and advancing well crafted policies, data governance, risk management, compliance, base security and operational practices are necessary. Licensing of information technology architects, IT systems and security engineers are recommended with mandatory education, training and licensure with well-funded and efficacious accountability regimes is recommended.

Technologies that process digital identities and related personal information should be engineered and deployed responsibly. Technology and service certifications should be created to ascertain and assure the quality and reliability of such technologies and identity and related information asset management services. Mandatory rating labels and notices to the public of identity and personal information processing technologies and services are to be created that inform citizens of the device or service assurance level and provide guidance on security, trust and privacy risks associated with such devices and services.

Organizations would apply for licenses to operate information utilities. Such operations will be inspected, audited and provided model contracts detailing responsibilities and liabilities that members and operators can negotiate limitations, ceilings and base remedies for violations of contract terms. Information utility operators will have the ability to choose to be self-governed and/or have inter-community oversight bodies with powers to resolve disputes, operating issues and enforce data protection authority orders. The state should institute a data protection commission made up of elected private citizens, information utility officers (or boards) and a data protection commissioner(s) who have judicial (California Supreme Court) authority and powers to adjudicate cases and establish license and operational standards. There should be a separation of powers and appeals process in place.

Profits, operating costs and revenues are under the authority of licensed operators and their oversight communities. Distributions of profits are solely the choice of operators and their member communities. The state may decide to tax information utilities or allow them and their member communities to dedicate funds for the greater social welfare of their member communities and the funding of oversight, adjudication and licensure programs. It would certainly be empowering for citizens to decide for themselves which ones, how much or whether they want to fund particular community programs, and to recommend and vote upon expenditures themselves. A self-imposed information utility tax of which citizen-owners' decide the use of such funds would be preferable.

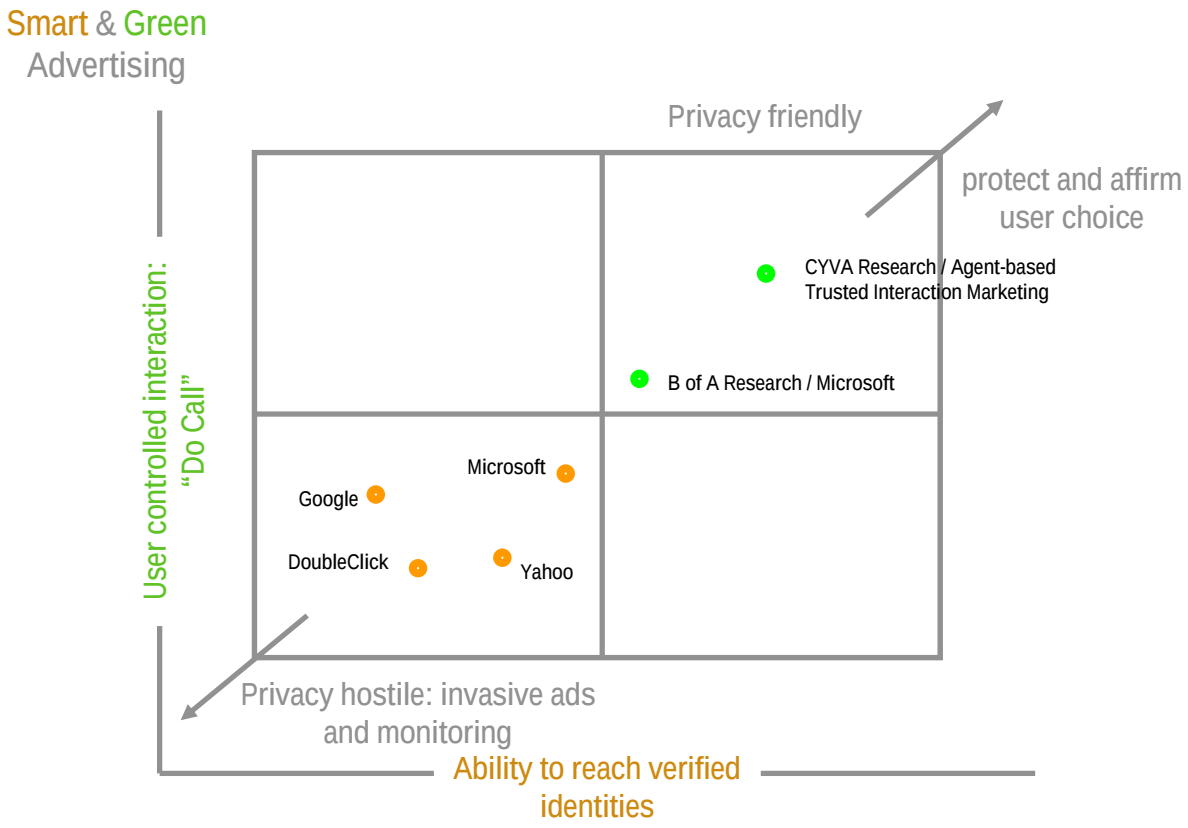
3. A Proposed Means for Change: Experimental Technologies and Services

The intrusive and coercive collection and trafficking of personal information is escalating. Many continue to suffer the onslaught of in-your-face hostility to “leave me alone” resistance. There is Paparazzi attitude and drive that coldly and callously reasons that it is okay to steal and abuse our human-digital being anytime they want and no one can stop them. Laws are to be ignored, because it is simply to expensive and difficult to enforce. This will change.

Another avenue, amongst several that are emerging in the realm innovative technologies and services is those proposed by CYVA Research. The following are technological and service-oriented systems that are described as potential solutions. Much of this work is experimental and still in development. The design and ambition is to empower and affirm the inalienable right of informational self-determination – our information privacy and the authoritative and assertive capability to command and control our personal information anywhere, anytime and according to their terms, derive value or benefit from the secure and trusted use of their personal information assets.

3.1. Smart and Green Advertising: Consumer Choice and Control

The value and effectiveness of advertising platforms is increasingly dependent on the trustworthy interaction of merchants and consumers. Advertisers want their ad dollars to maximize sales, reaching specific consumer segments and being able to monitor and adjust ads as they intelligently track effectiveness. Consumers on the other hand don’t



want to be unnecessarily intruded upon or have their entertainment experience polluted and hamstrung by unwanted marketing messages. Both parties want choice and control in merchant-consumer interactions; properly mediating such interactions is central to CYVA's Personal Information Agent, Trusted Network Community and Trusted Interaction Marketing technology and services.

3.2. Disruptive Advertising and Content Distribution Opportunity: Just Do it Right

Mobile TV is certainly disruptive as it creates a wholly new venue to offer rich media and effective advertising content to consumers. However, along side this potential is the reality of media over exposure and intrusiveness. Fact is many consumers love to be connected to entertainment content anywhere, anytime but vehemently object to being bombarded by unsolicited marketing pitches, especially on personal devices. The Federal Trade Commission has held numerous workshops in assessing wireless advertising and data services[9] seeking to assess the implications to consumer privacy and security, providing ongoing guidance to congress in considering new legislation to protect citizen-consumers from abuse.

Central to properly mediating the interest of advertisers, ad agencies, media distributors, content publishers, mobile carriers and subscribers is who controls and manages the interactions between subscribers and advertiser, especially the collection and exchange of consumer personal information so necessary to effective ad management. Advertisers want to know a great deal about subscribers but the trustworthy means to properly control and rightfully mange such personal information remains a challenge.

3.3. Experimental Technologies & Services: A Personal Information Agent for Asserting Citizen Privacy and Security

Central to advancing human-digital rights and responsibilities is the pursuit of experimental technologies and services that empower individuals and/or their chosen custodians to securely command and control their personal information anywhere, anytime, and according to their terms, derive value or benefit from the secure and trusted use of their personal information assets.

CYVA's solution is the concept of informational self-determination: the right of individuals and/or their legal custodians (e.g., parents, legal guardians, contract identity providers and information asset managers) to directly and assertively command and control their personal information anywhere, anytime. This is made possible by CYVA's patented self-determining digital persona (SDDP™)

technology that transforms data into intelligent self-protecting software, a Personal Information Agent™ (PIA™). This represents a fundamental paradigm shift in information assurance – making data self-protecting – able to protect and assert self. Data processing rules are portable and persistent, traveling with and bound to data. This technology is the basis for establishing a much needed new service provider: a Trusted Information Utility® (TIU®).

Our vision is to equip, train, and empower individuals to securely command and control their personal information anywhere, anytime, and according to their terms, derive value or benefit from the secure and trusted use of their personal information assets.

It is critical to our digital economy and information society that we address the out-of-control state of personal information (PI). The benefits of e-commerce and advantages of digital existence are now eclipsed by rampant fears and vulnerability; millions have suffered identity theft with billions lost by business and consumers. Phishing attacks, spyware, viruses, intrusive surveillance practices, compounded by the unfettered strip mining of personal data, are reaping a spiraling destructive erosion of consumer confidence and mounting angry reaction, with legal and regulatory consequences.

To restore consumer confidence and trust, CYVA Research is forwarding a much needed paradigm shift in how to secure and equitably manage personal and community-sourced information assets. The firm is forwarding a suite of user-centric identity and information asset management technologies and services that leverage key infrastructure partner products and services. These transformational offerings provide disruptive competitive advantages, strategically supported by the firm's international intellectual property portfolio.

3.4. Trusted Network Community Solution

Reputation is essential to brand management. Advertisers invest millions in building and maintaining brands. With the ability to extend that brand into new venues comes the challenge of brand risk management. CYVA Research's Trusted Network Community and Trusted Identity Management services provide a means to manage and control identity assets, the data, behavior or rules governing data use and the reputation of consumer and merchant community members. Through the use of Personal Information Agents both consumers and merchants can securely interact and perform trusted information for value or benefit transactions. This provides both parties a means to negotiate choice and control of advertising offers wherein specific targeted consumers can receive value or benefit in exchange for viewing or interacting with an ad agent. PIAStructures, a multi-agent ad structure, empower community-focused product or service offerings wherein specific communities of consumers and merchants perform aggregate information for value or benefit interactions.

Central to CYVA's approach to protecting consumer privacy and maintaining the trusted reputation of merchants is the trusted ongoing command and control of identity and personal information assets within the Trusted Network Community. Consumer Identity and personal information remains under the command and control of consumers and/or their Trusted Network Community operators throughout the personal information lifecycle. Identity or PIA types, namely anonymous, pseudonymous or fully identified with assured validity of personal information assets again are controlled by citizens

and/or their trusted custodians. This is essential in addressing consumer concerns, maintaining merchant reputation and a growing body of data protection laws worldwide.

3.5. TNC Operator Services

The firm's personal information security and identity management technologies form the basis for Trusted Network Community™ and Trusted Information Utility® services to be offered by TNC®/TIU® operators:

- Trusted Identity Services™
- Trusted Search and Selection Services™
- Trusted Interaction Marketing Services™
- Trusted Identity & Information Asset Management (I2AM™) Services

3.6. Value Proposition

TNC operators and advertisers benefit from a secure and trustworthy means to interact with consumers while fully respecting and affirming citizen-consumer human-digital rights and responsibilities (HDR&Rs). Do call and do not call preferences are dynamically changed at will affording advertisers and consumers a robust and powerful means to negotiate trusted interactions and remain accountable under agreed information asset processing rules. Advertiser can now enjoy a verifiable relationship with true consumers as asserted by TNC operators and identity providers. Mutual trust can now be the standard in chosen relationships amongst vendor and consumers with strong means to manage identity reputations for e-commerce.

TNC Operator and Advertisers

- New synergistic technology and services to enhance advertising effectiveness
- Expanded intellectual property portfolio in protecting and advancing domestic and international markets
- Trusted Interaction Marketing services to address growing security and privacy concerns
- Robust industry defense and protection of reputation e.g., data breach, ID theft
- PIA-based advertising to enhance and protect consumer-advertiser relations
- Subscriber and advertiser loyalty

Consumer Subscribers

- Strong protections in addressing consumer privacy and security concerns
- Personal information assets secured and controlled anywhere, anytime
- User-controlled identity management wherein consumers and advertisers negotiate identity processing rules
- Trusted social-networking and user-generated content
- PIA-based advertising to enhance and protect consumer to consumer interactions
- Greater confidence in being digital

3.7. Privacy Assertive Technologies: Always On User-controlled Identity

CYVA Research is one of several firms pursuing the concept of a user-centric identity or user-controlled identity. Use cases vary in what is the intent, scope and purpose of user-controlled identity. Past efforts to pursue privacy *enhancing* technology have provided a collection of approaches; however, it is becoming more apparent that once a piece or collection of authorized personal information is released how do you continue to assure proper use and protection from abuse. To this end privacy assertive technologies aim as a means to command and control data post exchange and beyond, namely a continuous assertive compliance with a data subject's rules.

3.8. Addressing the Competitive and Cultural Realities of Innovation and Impact to Our Human-digital Well Being

New technologies continue to erupt and displace the old. Mobile TV, social networks, cars that know us our whereabouts and can quickly marshal emergency resources at the press of a button. Phones with 5 Megapixel camera, and GPS capabilities that can capture real-time images and instantly send them over broad-band networks are impressive but spooky in that getting caught in compromising circumstances can now be shouted 'hey look what I caught on camera' to the world.

What is clear is that time, date, and geo-location stamping of captured visual content is possible and what this can be used for is a whole lot of innocent fun and reasonable benefit but also a world of hurt, but that depends. With mobile TV and instant capture and sending of video is even cooler or chilling given I might capture a video of friends, post it on some social-network and later be standing in court with parents asking what was I thinking in exposing their daughter to a bunch of 20 something males operating as a pack, sharing techniques and targets of young adolescent females. This is not fiction but a dark reality of social-networking that state AGs are aggressively pursuing need changes.

This innovation of video enabled phones offers fresh advertising opportunities empowering a mobile TV advertising experience; but these ad revenue driven technologies should responsibly address the growing quandary of personal security and invasive abuses of our privacy. Consumers world-wide and law makers are on edge with regards to privacy and security. As fantastic as the real-time delivery of video on mobile devices represent our present hostile and toxic digital ecosystem has significantly tainted the consumer experience and without properly addressing this reality consumers and advertiser may not eagerly embrace the benefits of Mobile TV.

What is necessary is a means to secure and control user-generated content. Sensitive data can be securely captured from device processors and encapsulated within Personal Information Agent technology that binds default governance rules to protect user-generated content and enforce rules that are always on. Syncing and setting permissions from joint owners or custodians (parents) of content is preferred and is necessary means to authorize, affirm and enforce identity and information asset rights and responsibilities.

4. Conclusion

Information technology invention and how such inventions are employed must more carefully consider social consequences and be governed by and held accountable to a set of value-conscious design[10] principles. Where there are conflicts of interests in how a technology is designed and employed we must put into place a more thorough and effective means of discovery, challenge and resolution. Corporate interest in maximizing and maintaining power and profits at the expense of citizen privacy and security is unacceptable. Citizen backlash is visible everywhere but the dysfunctional political apparatus and its bent towards self-aggrandizement is stifling meaningful change.

Our present political-legislative process is broken. However, the underlining constitution (U.S.) and principles are sound[11]. I argue that a Natural Law inspired, citizen affirmed and citizen-controlled digital identity: their protected information being and assets, can greatly affect our economic and political process. We the people can better influence and steer the participants and the process towards a more faithful adherence to moral code and values we cherish and hold dearly as an information culture and global community. This is a potential, an opportunity, so that we may more effectively protect and enjoy the benefits of a free and secure human-digital existence.

Notes

[1] Slavery is still secretly practiced in parts of the world today. Howard Dodson. “Slavery in the Twenty-First Century,” UN Chronicle Online Edition. http://www.un.org/Pubs/chronicle/2005/issue3/0305p28.html

[2] In 1983, in response to a controversial national census, the German Federal Constitutional Court issued a decision that established Germany’s current legal concept of privacy. The doctrine of “Informationelle Selbstbestimmung” (informational self-determination) states: “This Fundamental Right insofar authorizes each individual to determine on the circulation and the use of his own personal data. A limitation of this Right on ‘Informational Self-Determination’ will only be allowed in the case of prevalent public interest.” Accordingly, "the protection of the individual against unrestricted inquiry, storage, use, and circulation of his personal data” is a constitutionally derived and fundamental human right in German law.

[3] J. Budziszewski, “Written on the Heart: The Case for Natural Law” InterVarsity Press, 1997. “According to Locke, the condition befitting the nature of men is “a state of perfect freedom to order their actions and dispose of their possessions and persons as they think fit, within the bounds of the law of nature, without asking or depending upon the will of any other man”. Notice that freedom means not having to take orders from a master; it does not mean being able to do whatever I please.

[4] Daniel J. Solove, Marc Rotenberg, Paul M. Schwartz, “Information Privacy Law” Aspen Publishers, 2006. pp.184-186.

[5] Jonathan Dolhenty, Ph.D., “An Overview of Natural Law Theory”. http://radicalacademy.com/philnaturallaw.htm

[6] J. Budziszewski, “Written on the Heart: The Case for Natural Law” InterVarsity Press, 1997. pp. 123-125.

[7] European Data Protection Supervisor, “Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive”, July 2007. http:// www.edps.europa.eu

[8] International Security, Trust & Privacy Alliance, “Analysis of Privacy Principles: Making Privacy Operational”, 2007. http://www.istpa.org

[9] The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues Federal Trade Commission, February 2002. http://www.ftc.gov/bcp/reports/wirelesssummary.pdf

[10] Michael T. Zimmer, “The Quest for the Perfect Search Engine: Values, Technical Design, and the Flow of Personal Information in Spheres of Mobility”. Program in Media Ecology, Department of Culture and Communication, The Steinhardt School of Education, New York University, 2007. http://michaelzimmer.org/dissertation/

[11] Judge Andrew P. Napolitano, “The Constitution in Exile: How the Federal Government has Seized Power by Rewriting the Supreme Law of the Land”. Thomas Nelson, Inc., 2006.