Digital Justice & Social Security System

Digital Transformation Infrastructure requires Systems & Solutions for Justice, Digital Prisons, Social Security & Protections of Human Rights

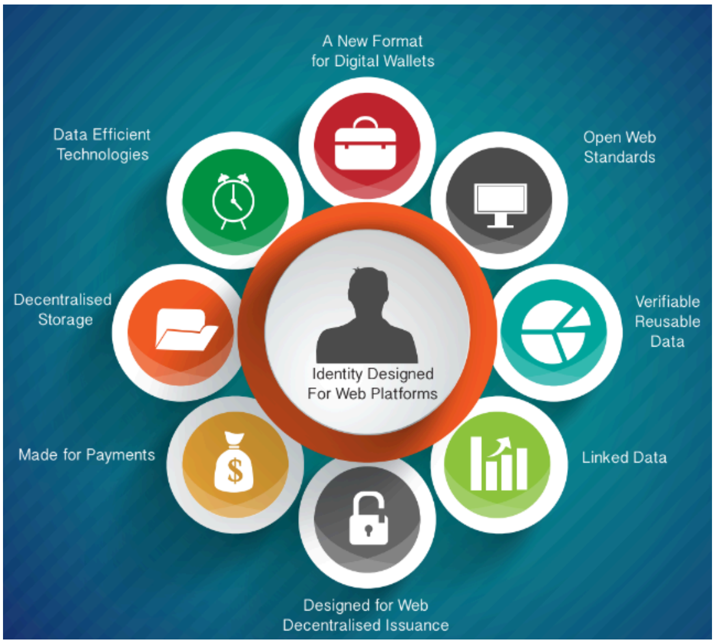


Image Source: 13th May 2015 Trust Factory Slides for Government to register the trading name Trust Factory,[1] to advance 'credentials'[2][3][4]

---

[1]. https://drive.google.com/file/d/12iVsYFhjRMKyuq1DqtfU51Kr0YSdsx7q/view?usp=sharing

[2] https://drive.google.com/drive/folders/1lV-Ruj9Gehwvs7B3wDLd6fmKIlvCmOqt

[3] https://www.w3.org/community/credentials/2014/08/06/call-for-participation-in-credentials-community-group/

[4] https://soundcloud.com/ubiquitous-au/credentialscgtelecon2015-06-02medical

This document is a work in progress.... Productive Contributions Welcomed.

The mailing list is: https://groups.google.com/g/peace-infrastructure-project

FB Page: https://www.facebook.com/ThePeaceProject

FB Group: https://www.facebook.com/groups/757084252017425

Research Library (google Drive):
https://drive.google.com/drive/folders/1tYFIggw8MIY5fD2u-nbwFRM6wqrhdmQZ

Discord: https://discord.gg/CpXecK6jMu

NOTE: W3C Human Centric AI CG was established on the 4th April 2023, efforts are now being made to modify this document to better support the now somewhat shifted scope & intended Audience, et.al.

https://www.w3.org/community/humancentricai/

Table of Contents:

Table of Contents: 2

- Preface 3
- Summaries 3
- History 7

Introduction 9

- The Implications of AI 11
- The Broader Lens 16
- Social Protections Structural modelling. 20

Justice Infrastructure: Human Rights & Rule of Law 21

- Technical Solutions: Standards - Past, Present & Emerging 25

Formalisation of Cyber Justice Infrastructure. 27

- Support for Separation of Powers 31
- Associative Analysis of UN Instruments for Online Systems 31
- Further Reading 32

Related Works 34

Codename:Safe t(ech) net 34

Regulation - Design considerations 39

Safety Protocols 41

Social Attack Vectors 42

Introduction 42

Discrimination based attacks. 53

Dishonesty 55

Cyber Attack Vectors 55

Digital Slavery 59

MisRepresentation 64

Nobody AI 64

Tech Debt 65

Permanent Identifiers 66

Strategic Harms & Exploitation 67

Torts 82

Economic Torts 85

Intentional Torts 86

Negligence 86

Nuisance 87

Criminal Activity 88

Corporate Crime 89

Environmental Crime 90

Financial Crimes 90

Fraud 91

Proxy Attacks 92

Safety Protocols 93

Background: Introduction 94

Agent Labelling 97

Freedom of Thought 107

HumanCentric Digital Identity 108

Human Centric AI 109

Values Credentials 109

Protecting Children **115**

Definition of 'Adult'; safety for persons who are 18-25? 116

Relationships (Social) **117**

Fair Work Protocols **117**

About the 8-Hour Movement 118

ESG Implications 121

Ending Digital Slavery **121**

Notes and Considerations 122

Knowledge Qualification Methods **123**

No Lock-ins **124**

Golden Handcuffs 124

Data Portability **125**

Solid & Similar 125

Enforceability of Rules 126

Banishment & Exile. **127**

Guardianship Semantics **129**

Introduction 129

Guardianship Relations 130

Community of Practice **138**

BestEfforts 139

Fit For Purpose 140

Learning Modals 141

Temporal Semantics 143

Preface

The project is considered to be part of the ‘Peace Infrastructure Project’, Scope of works.

In-order to support exponential scalability of productive works, a means to ensure safety of persons and support for human rights is a necessity. In-turn also, there are many locations where the means for people to have their own ICT infrastructure is unlikely; as such, these persons need infrastructure to support their human rights in the absence of alternatives.

The way in which many works are done for civics (classified as ‘Web Civics’ works) is in the open. Therein, there’s a process - and the method also invites others to contribute, although that is not often meaningfully the case.

Personally, I find the process - when seeking to address difficult issues, somewhat - emotional, and I'm quite sure that ends-up in text, particularly in earlier drafts, than is otherwise the case once works have been more fully processed to outcomes.

The experience of thinking about something that doesn’t exist, and then discovering the potential impacts and implications; upon so many people, both, a meaningful and emotional experience; whilst thinking - at least, i’m associative enough to do it, where so many dissociative workers in gainful jobs, have otherwise failed to do so, or so it seems.

There are many areas of intersectional consideration between the influence of technology upon society; and the findings identified via analyses of the characteristics of what does & does not exist. When considered, and to some degree assessed, the implications can often be profound.

The creation of this document, started with the idea that - whilst challenging, engaging in the concept of defining digital prisons for those who should be, or simply end-up being, subject to authoritarian punishments online - should be formalised, as even prisoners have rights. The implication being, that whilst action on supporting the human rights of persons not suspected of a crime - may be considered too hard, contestable and/or subject to politics in debilitating ways, the means to define rights for prisoners - would in-turn lead to outcomes for all persons.

In-turn, this brings about the need to consider how to support the human rights of people subject to actions; including, the means to retain and ensure the ability to present evidence.

This in-turn leads to an outcome where, most likely, the means to ensure portability of information in systems, in a manner that does not unduly injure the useful employment of systems, in a manner defined to be allowed by courts of law, etc… may in-turn, invoke various requirements as to ensure local administration of law, or in-effect support for rule of law, which may in-turn be usefully employed by all persons; in ways that have previously been unavailable.

Whilst there are many calls to act and address the issue of online crimes, this is a means to do so; as such, would the opportunity to do so, be taken-up - or is the call for systems of justice, more about pervasive surveillance and the diminishment of human rights, rather than the protection of those rights; as is sought to be the approved outcome, in the quorums of the UN.

As such, the foundational requirements for justice; include but are not limited to, infrastructure akin to prisons or ‘cells’, for those whose activities are alleged to warrant lawful purpose for electronic confinements and related measures.

Thereafter, the implication becomes also, the means to support those who are serving a sentence, which then leads to the means through which others may be distinguished, and the rights of persons who are not subject to lawful interference; as well as, the means for those who have been falsely accused and/or harmed, to be furnished with the capacities required, to support natural justice.

These considerations are in-turn considered to be vital for the future of how it is that we define appropriate cyber-security infrastructure, as to ensure we connect - what people do - to the effect, of actions; whether they have been taken by an agent on behalf of legal and/or natural persons, or as a group; or whatever the circumstance, without pre-determining guilt, the test environment, should it be required and when required; is a court of law, that has particular requirements, that are either supported - or they are not, by design.

Should this exist, one might hope that more people seek to ensure that they’re actions do not result in court-related judgements, and perhaps - this in and of itself, may have a dramatic impact, upon the behaviours of all people.

However, from this initial perspective; the scope, then expanded somewhat, taking into account various threads that becomes part of an ecosystem that more wholly considers and / or presents, the various related considerations and implications; as may in-turn, be better considered as a broader embodiment, notwithstanding the underlying requirement - prisons.

I have folded into this document; works done earlier on both social attack vectors, and safety protocols - intended to address the risks / threats; as well as other historical works, that relate to the same field of consideration, including but not limited to, social security & safety systems.

Whilst this is not exhaustive, and i’m sure i’ve got more in the archive (inc. consideration about people made homeless, domestic violence victims, and alot more); i hope, this helps for now.

Finally; over the past few weeks, I have had some involvement as a participant in international works defining our shared digital future; which was in-part, what stimulated the initial efforts on this document.

In-turn, I have also instigated the establishment of a W3C CG to focus on Human Centric AI requirements; which may in-turn, act to work with other W3C groups, to define technological standards - useful - for addressing some of these problems, although not exclusively.

My efforts are self-funded, on a meagre income; that both, has the effect of worsening my circumstances whilst living under the poverty line funding costs, of existing with purpose in life; as I continue this very challenging pursuit, working to support human rights via “Web Civics”.

My Background:

I have placed a bit of a background about me at the end of the document.

Suffice to say, I was involved in developing the technology, in its early stages, that is now used foundationally, world-wide. From my point of view, these works were required constituencies to an effort to create something - whilst working in a manner that sought to protect human rights of persons, particularly the most vulnerable; and those, in complex situations, involving complex issues.

My desire, efforts and sacrifices were intended to produce systems to support human rights, presently, the consequential outcomes of how they have been commercialised, do not do this.

It was reconciled by Feb 2020, in what was a rapidly and poorly drafted submission[5] in the hopes that the circumstances could be positively influenced, in what was a lost-cause.

Now, that the first wave of agents commercialising their version or variant of ‘digital identity’, FinTech / AML / KYC and related infrastructure has been executed, there is now an opportunity to distinguish my intended purpose for the works; offerance for those who seek to support ‘reality check tech’ and the infrastructure needed to support it.

This includes; ensure interoperability between systems that are made with different ideologies, whilst simultaneously also seeking to ensure that whatever people find themselves dependent upon, human rights considerations - even for real-world or digital refugees, and prisoners - is able to be supported. Fundamentally, the body of work is ‘mission based’, whereby should the outcome be successfully delivered, then the useful employment of it - will be a form of apparatus that supports human dignity, both, for the honourable & those who do good work.

At its core is the desire to employ sophisticated capabilities to protect the human rights of children from all adults who may otherwise seek to gainfully exploit and consume those rights.

More than a decade down the track,with some derivatives now deployed upon billions of people; these core objective purposes still remain - beyond the scope of others priorities, as is demonstrably illustrated, by the exhibit of what does exist; and indeed also, what does not exist.

---

[5] https://drive.google.com/file/d/1leNX8bjTG-XLNgkuRyMhljjpTIF8KoHA/view?usp=sharing

Summaries

There are a couple of primary forces that have led to the production of these works, the first is about the nature and purpose of my work, for over a decade; whilst the other more recent events are two fold,

1. The Need to have a platform to send people to if they are exiled.

   The "Human Centric AI" systems work, evolved from work to build a particular type of implementation that i call 'webizen', thereafter, one of the 'safety protocols' is the means for host providers to boot a customer off their network; whilst noting, that the methodology is subject to lawful review and consequence, if done for improper purpose.

   As such, there needs to be a 'platform' solution that can be used by people who are booted off other solutions, otherwise available on fair-terms or otherwise.

2. Participation in WSIS
   I recently participated in WSIS2023[6][7]. There were various topics, and consequential considerations that led me to believe that an approach to form a solution for a digital prison system; and thereby also define the rights of prisoners, is a matter of importance.

   The implication being, that by defining the rights of prisoners, the rights of free persons otherwise not accused of a crime / subject to court orders, becomes instrumentally defined also. The broader implications thereby also lead to a significant broadening of the platform definitions already implemented, as to support human rights & rule of law.

The document is presently taking form as a personal work, as a consequence of me personally doing it. It is expected that derivatives and/or future drafts, may attract the assistive contributions of others as the project takes shape, and that therefore the personal aspects should be stripped from it - but that's not part of my initial methodologies.

Thereafter, as i reflected upon the the various considerations and related works, as do in-turn provide resources to construct the constituencies to this broad concept; that in-turn needs to form into a comprehensible, cohesive ecosystems solution framework that is in-turn able to be updated, adapted, improved upon, etc; i thereafter, added various other elements to the brief.

Should, the underlying considerations considered to have merit,

---

[6] https://www.itu.int/net4/wsis/forum/2023

[7] https://play.itu.int/events/category/wsis-forum-2023/2023-03/

Initial Requirements: To Support Progress

a. An Environment / Venue; for cooperative works to establish the foundational use-cases, requirements and various other considerations - needs to be established.

b. A call for participation needs to be made; and subsequently, provided administrative support required to process the volume of work associated to the undertaking.

c. The broad array of examples and use-cases needs to be identified and documented.

d. An assessment of the applicability of statements in human rights instruments needs to be assessed, through the context of how and what functionality matrices need to provide.

e. Communications materials to illustrate the features and functions of the technology solution, and how it is able to be employed by various online systems (inc. import/export) is in-turn required.

f. The rules need to be defined and/or made definable.

Objective Milestone.

The objective of this project is to reach a point where the information is provided to the Global Digital Compact and other related UN associated stakeholders, to define the electronic human rights of persons - particularly therein 'prisoners', as is expected to be applied for digital transformation agenda / SDG related works. The Technology platform illustrated; solid, is defined as W3C open-standards and can either be implemented by platform providers via new or existing solutions. There are presently large-scale implementations, providing 'pods'.

The greater challenge is thought to be ensuring support by platforms in a fit and proper manner. It is expected that some will provide support, whilst others may elect not to, for whatever reason.

These works implicitly introduce support for Human Rights as part of the Digital Transformation, Global Digital Compact and related SDG associated international works.

By defining how it is that prisoners should expect to be treated with respect to their electronic information systems, the implication becomes one where the rights of free persons must also be considered. There is an overwhelming desire to address online crimes, as a priority.

Technical Summary

The suggested technological foundation for a solution is suggested to be SOLID.

What is Solid

A matter of great importance is the ability to understand what 'solid' refers to. Solid is a body of work, produced into open standards, as an embodiment of various constituencies via the W3C that provides an open-standards based platform for the operation of information in a manner that functions in a decentralised way.

The website for the solid project is: https://solidproject.org/ with the specification being defined: https://solidproject.org/TR/protocol

“Solid has become the vital next layer of the web stack.”

- Sir Tim Berners-Lee

“Solid has extended the web to include identity management, access control and universal standards for data. These capabilities decouple data from applications so that data is organised around individuals.”

Source: https://www.inrupt.com/solid

Solid, was historically called RWW[8], various recent press articles can be found,

https://www.inrupt.com/coverage and in-turn also, https://twitter.com/inrupt

The earliest record found, so far, of Tim Berners-Lee talking about semantics and the relationship between the design of the web and the conscious experience of persons / reality, is from 1994. A snippet of a longer-form piece of media has been created, as is available via this link: https://www.youtube.com/watch?v=UkjyCPuTKPw

In-order to support the means to form a ‘digital prison system’, and in-turn support various other use-cases that have similar sorts of requirements; as to protect the human rights of all persons, it is my belief, presently, that solid works, as led by Tim Berners-Lee is a solution.

Summary Re: Sold

Over the course of the last decade, many solutions for personal data storage have been produced, including solid and works undertaken via the My Data[9] initiative, internationally.

Yet, the expansive requirements to ensure the means to ensure a portability methodology and governance framework, seemingly still needs more work to be implemented.

In-part, this is also required to ensure deplatforming actions do not invalidate a persons rights other than as is required to remove or exile a person, from a platform for reasons best sought to be equipped for review by a competent tribunal or moreover, a court of law.

In consideration, Solid is considered to be the best available solution that is considered ‘fit for purpose’ is the technology platform produced via W3C groups, called Solid. Inrupt / Solid, has demonstrated itself to be equipped to support governmental implementations[10], and as such this is something they are thought to have demonstrated capacity to achieve. As such, a

---

[8] https://drive.google.com/drive/folders/1lpeoEFowRcq3VTAp5LH6cFN251O9g9iE

[9] https://apply.mydata.org/gallery

[10] https://www.inrupt.com/blog/flanders-solid

means for information to be exported in a useful and functional format is already 'in production', in a manner that has been defined through the use of open technology standards methodologies.

This in-turn leads to considering a series of requirements to ensure that platforms provide interoperability in a manner that supports chain-of-evidence, as is thought to be a foundational, practical - technological requirement.

Other associative considerations include augmentation of existing technological solutions for what is now called 'verifiable credentials' whereby agreement between agents online should empower ALL participants to define terms (ie: human rights terms) that they intend to honour.

Whilst it is entirely likely that not all platforms will voluntarily consent to providing support for what is effectively a means for portability of users, who are otherwise locked into platforms, the means to provide badges that show which platforms do support these features and which do not, could be defined. This in-turn requires a - properly - decentralised method to support how any such form of 'credentials' / 'open badges' can be issued and/or managed, reliably. Whilst the intended purpose is to provide safety, the implication if poorly defined, may worsen circumstances of people targeted and/or sought to be exploited, by others. As such, a cautious approach is sought to be employed as methodologies to define approaches, are in-turn defined.

By the creation of solutions and in-turn also, specifications - that can be employed to provide these capabilities; the emergence of market based alternatives may act to meaningfully support, human rights for those who seek to exist both; with the personal responsibility to attend to the meaningful implications of those considerations, and in-turn also the benefits. Whilst broadly otherwise, providing a formal means to support human rights related functional requirements whether or not users seek to uphold, protect or respect the considerations made by them; and in relation to them, the outcomes that may therefore be defined in courts-of-law, related systems of justice, social-security and safety measures.

Social Factors Summary

There are a great many challenges associated with human rights, including but not limited to rule of law and protection of persons from exploitation, crimes and other forms of wrongs; including but not limited to, revocation of natural justice, related requirements, and apparatus.

There are various use-cases where a digital justice system, that provides support for use-cases; that include but are not limited to,

- Detention (electronic or physical)
- Storage of electronic evidence
- Digital and/or physical refugees
- Protection of persons from online crimes & (alleged or obvious) criminal activities.

Others include also,

- the needs of persons who are physically serving time in correctional facilities,
- the circumstances of persons who are deceased,
- those who require safety protections,
- access to justice,
- temporary or permanent guardianship; and/or,
- Policies required to support means to gain access to evidence required to provide lawful remedy.

The undertaking requires procedural considerations about how to support the human rights of prisoners, even those who are found guilty of the most heinous crimes.

These considerations thereby also extend to those who are suspected or accused of wrong-doing in some way that may lead to online punishments being delegated by platform agents.

The ability to define whether or not someone is a criminal and/or has a criminal history, particularly in circumstances where any such charges are not dismissed and/or exhausted (ie; a person has served their time); is as important, as ensuring that systems provide support for rule of law and that any person engaged in harming others for gainful purpose, wrongfully, is able to be brought to a court of law, by the victims of any such crimes; as is vital for all (human) rights.

Today, there are many significant challenges associated to pursuits to address online wrongs & crime. Some may reasonably argue, that there is a very high degree of lawlessness and the impacts of criminal activity of various kinds, disaffects our world, our communities, our capacities and our use of resources.

The site 'dataprod' notes[11] that an estimated 85% of all email is spam - as such, the volume of CO2 created by only this problem is significant.

It is thought that the biggest contributor to harmful climate change CO2 emissions that can be addressed comparatively easily, is corruption; which if addressed, may in-turn lead to improved capacity to address various other issues of great impact and concern.

The ability to deliver solutions to improve the quality of life of all members of our human family who are not otherwise engaged in serious crime; could be radically improved, by our ability to ensure that all persons are equipped to positively contribute towards the definition and creation of solutions, with dignity, to address the many issues of a serious nature; whilst being paid fairly for any useful efforts made to do so, as protected by law.

---

[11] https://dataprot.net/statistics/spam-statistics/

Quick History - How the concept came about…

Credentials Go To the UN

W3C Credentials Technology started with the foundational requirements for web-payments[12], which in-turn led to IGF sessions september 2014[13][14], which I attended remotely (although the transcript misspells my name 'hallborn' or similar. As the web-payments work progressed, the credentials component was separated via the creation of the Credentials work, first applied upon 'verifiable claims'[15]. I remember providing updates, but didn't get any feedback[16].

In the beginning, the use of the credentials works was about 'verifiable claims' & credentials, as noted 2nd June 2015[17], like a 'washer' that goes onto a bolt, or in this case - electronic documents, so that they are provided the properties required for artefacts to be employed as evidence. The story about that concept, from my perspective relates to an old story i was told;

Once upon a time, A comment was made to me about the memory of a story that a large automotive parts business called, and how it was born due to some sort of patent or ownership over washers, that go onto bolts as essential items… don't own the car, own the 'washer'. Well in a similar way, if the outcome was to protect freedom of thought, this essential component needed to be part of the patent-pool protected open-standards.

Yet, when they reached the UN, that i do not recall being made aware of; and couldn't afford to attend in anycase, Credentials was highlighted as a means to support the needs of refugees and SDG 16.9[18].   These sorts of considerations were a concern, as the WebID community had important ecosystem components for providing support for 'identity', that I advocated for Credentials as a means to compliment, rather than replace or act as an entire alternative. Noting that works in W3C is about creating open-standards, not specifically applied use-cases. Nonetheless, overtime, it developed[19][20], and by 2020, the use-case definitions were updated and Covid[21] provided the leading use-case for wide-spread implementation via the introduction of vaccine credentials and passports[22][23][24].

---

[12] https://cdn.knightlab.com/libs/timeline3/latest/embed/index.html?source=1Kab5bDqGkCGwkOUlAQ8NNlNUUBBVyzXQaYS9q6jLDZo&font=Default&lang=en&hash_bookmark=true&initial_zoom=3&height=900#event-universal-payment-for-the-web

[13] https://www.youtube.com/watch?v=m8cIYzy5MIA

[14] https://igf2014.sched.com/event/1k5zj4K/ws69-the-payment-privacy-policing-paradox-in-web-payments-systems

[15] https://drive.google.com/file/d/1Hc2h27likRBsqwjjRFTP6sA6ARqAq0Nl/view?usp=sharing

[16] https://docs.google.com/document/d/1GCFSwPPXjyZQukFhMzjGlfP-rSIFRO-nX4CTs6oWZD8/edit?usp=sharing

[17] https://soundcloud.com/ubiquitous-au/credentialscgtelecon2015-06-02medical

[18] https://indicators.report/targets/16-9/

[19] https://id2020.org/

[20] https://identity.foundation/

[21] https://covid19.who.int/

[22] https://www.prnewswire.com/news-releases/worlds-airports-and-leading-airlines-join-commontrust-network-and-begin-roll-out-of-commonpass-in-december-in-support-of-safer-border-reopening-301179752.html

[23] https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201920200AB2004

[24] https://web.archive.org/web/20201127144250/https://www.iata.org/en/iata-repository/pressroom/presentations/travel-pass/

“By April 2020, about half of the world's population was under some form of lockdown, with more than 3.9 billion people in more than 90 countries or territories having been asked or ordered to stay at home by their governments” source: wikipedia[25].

The need for persons to use broadband in ways previously unnecessary, acting to accelerate the implementation of the Digital Transformation Agenda[26]. The The State of Broadband 2022 report[27] Executive Summary[28] states,

> *“In 2020, the first year of the pandemic,* ***the number of Internet users grew by over 11 per cent****, the largest increase in a decade; in low- and middle-income countries (LMICs)* ***Internet use went up 15 per cent****. According to the latest ITU data,* ***Internet use grew to 66 percent of the population in 2022, reaching 5.3 billion people, up from 54 per cent in 2019****. A significant part of this growth was driven by the need to use quarantine related applications such as videoconferencing for work and education as well as online shopping, access to public services and remote health consultation. At the same time, the pandemic sharply magnified the consequences of the digital divide and today 2.7 billion people are without broadband and not able to access public services or learn from home.”*

The population forecast statistics from before 2019 to post 2022, were seemingly not subject to serious negative downgrades, at least not yet[29][30][31], as the consequence of choices will better illustrate overtime. Yet moreover, the implications of how these instruments are to be employed, will have a significant impact on the capacity, means, methods & implications of all SDGs related works.

There remains many human rights related use-cases that appear to be either, under developed, broadly unknown / not considered or absent.

During the pandemic, people whose lives were subjected to serious strains; locked into their houses, if they could continue to afford them, whilst tightly controlled by what they could say online to anyone, gave rise to various forms of speculation. As there is no formal digital prison system defined, the threat becomes the implications of global privately operated prison systems, whose activities are in-effect ‘above the law’.

As without a digital prison system, there is no meaningful capacity to make a distinction between people who are subject and/or convicted of crimes - as defined by laws; the alternative makes no distinction, which in-turn, perhaps, begs the question - is the internet itself a prison?

In-order to protect human rights, the question becomes - how to address the problems, the use-cases relating to wrong-doings, and in-turn also; ensuring human rights, even for prisoners.

---

[25] https://en.wikipedia.org/wiki/COVID-19_lockdowns

[26] https://thedocs.worldbank.org/en/doc/805211612215188198-0090022021/original/GovTechGuidanceNote1TheFrontier.pdf

[27] https://www.broadbandcommission.org/publication/state-of-broadband-2022/

[28] https://broadbandcommission.org/publication/state-of-broadband-2022/executive-summary/

[29] https://www.un.org/en/development/desa/population/events/pdf/other/21/WPP2017_press.briefing_Directors-web.pdf

[30] https://web.archive.org/web/20190404103020/https://www.un.org/en/sections/issues-depth/population/index.html

[31] https://www.un.org/en/global-issues/population

The objective belief is that by defining how the international digital prison system should work, from an international perspective; the practical implication will lead to, processes to define the human rights all digital prisoners and otherwise more broadly, all real-world prisoners should expect; which in-turn leads to the contrasting rights held by persons otherwise; as something, that is sought to be defined, as to render resolute support for the underlying UN instruments, without which, there would be no good purpose at all, for the UN.

If the struggle to provide Human Rights for all free members of our human family is too hard; then as a minimum, we should define the human rights that should be afforded to prisoners.

Thereby associatively considering the rights associated to people punished by others online; and the rights of persons who are subject to criminal proceedings and/or sentences, in the real-world; and what rights they should have to retain the digital artefacts pertaining to their lives; as well as the many other use-cases that may relate to any such form of infrastructure use.

Introduction

The document considers aspects relating to the notion of a digital prison system; and in-turn other digital justice and social-security use-case requirements for online government platforms.

Through the growth of international efforts, the development of various government technology platform works have developed significantly over recent years. Some examples of these works include the GovStack[32][33] works, and the works of the Digital Public Goods Alliance.[34]

Efforts are underway now to support the growth of technology for democracy and human rights[35][36] The existing works that have been produced over the past decade, now need to be updated to support human rights, including those who are reasonably imprisoned.

The ‘digital prison systems’ considerations are intended to provide a distinction between those subject to orders & those who are not; thereby, providing means to improve support for rights of persons not otherwise subject to proceedings and/or actions against them; and to preserve the rights of digital prisoners by way of formalised systems, and related considerations now made far clearer due to consequences of what people experienced during Covid.

---

[32] https://www.govstack.global/

[33] https://play.itu.int/event/wsis-forum-2023-govstack-cio-digital-leaders-forum/

[34] https://digitalpublicgoods.net/

[35] https://play.itu.int/event/wsis-forum-2023-technology-for-democracy-lessons-learnt-and-the-way-forward-for-technology-for-democracy-and-human-rights-1st-segment/

[36] https://play.itu.int/event/wsis-forum-2023-technology-for-democracy-lessons-learnt-and-the-way-forward-for-technology-for-democracy-and-human-rights-2nd-segment/

By defining a justice, social security and fundamentally also, digital prison system - the activity requires the need to clearly define the human rights of persons, as even prisoners have rights.

Those who are free, should not be subject to wrongs, particularly by those whose works (which relates to CO2 metrics) are funded by the government, or more specifically therein - taxpayers, citizens. This is expected to both act to address the enormity of the impacts corruption has up-on our environment and as a consequence of the vast amount of attributable CO2, which if corruption costs are measured by the some measures of the cost of a tonne of carbon, results in about 260Bn tonnes per year; even though the total carbon output, is about 20% of that figure[37]. climate change and our ability to achieve the SDGs, requires 'reality check tech', built upon systems that take into account what people do, and how it is that we consume energy; as may in-turn be considered, through the evaluation of lifecycle costs from cradle to cradle or grave.

Should systems continue to be defined in such a way that has the effect of interfering with the lives of persons, without available lawful remedy; including but not limited to acts of 'false imprisonment'; or any other act that may seek to cause injury to a target and/or invalidate rights; including but not limited to, those pertaining to a natural justice, SDGs cannot be achieved nor is it thought to be compatible with the UN Charter & various related objectives.

By defining 'digital identity' systems, where no proper support for systems of justice, as to protect against the misuse of technology as a consequence of how designs function already; The means to clearly define wrong-doings online, is presently unclear.

Today, people are judged based upon how much money they have, not how they got it, by design?

It is also unclear how the primary legal means of support for defining the terms upon which one-another engage in activities socially, commercially and otherwise online; is presently defined, to ensure that people are able to meaningfully participate in defining the terms of legal instruments associated to them and their lives through the use of Digital ID & Contract Law.

In considerations, by seeking to define how to define and protect any remaining rights of those who are accused or prosecuted & convicted of even the most heinous crimes; then the means to address what rights apply to all others, becomes part of a matrix brought about due to attention.

The implications brought about when a person intentionally restricts another person's rights and capacities via Information Communications Technologies, without appropriate legal authority to do so; and/or, in a manner that acts to harm persons without a reasonable basis to do so; as should otherwise be equipped with unfettered availability of electronic evidence for consideration by a court of law, using the same infrastructure needed for prisoners, is not done.

---

[37] https://ourworldindata.org/greenhouse-gas-emissions

Without well considered means to appropriately define lawful penalty and/or interference with the rights of free persons, otherwise not convicted of a crime nor subject to court proceedings, implications continue to engender prejudicial circumstances that act to influence our future.

And; the means to address various cyber-crime related issues becomes seriously impaired, which raises many threats as the development of Advanced Quantum, AI, IOT tools grow. Effort to ensure the means to distinguish between those lawfully subject to prosecutorial punishment & those who by law should be free, have rights; the means to distinguish & employ law is required, in a manner that is not clearly otherwise considered, to already be in place.

By forming a system for the administration of justice in support of the digital transformation agenda, the infrastructure requirements give rise to support for providing infrastructure for other broader social-security use-cases, expected to be required to support safety of persons & rule of law. In-turn, this is considered to be of particular importance with respect to our joint capacity, to work as an international human family to deliver the best possible outcomes for billions of people world-wide whose lives presently exist suffering from a lack of resources; such as to include, issues with respect to food supply, water, medicine, opportunity, energy & technology for education, learning, safety & thrive-ability of local biosphere ecosystems.

At one end of the spectrum, there are reports of problems even with peacekeepers[38], and whilst trafficking related problems[39] are amongst the most heinous crimes, at the other end of the spectrum is a desire to build billions of homes, improved socioeconomic & biosphere environments to radically improve the lives of people; which depends upon the money going to the right people for good purpose; not people with power, committing serious crimes, abuse.

Works on 'digital identity' solutions have been on-going since before 2000, from 2012[40] onwards[41], governments have been collaboratively defining 'digital identity' solutions as part of the requirements of digital transformation infrastructure via UN SDGs[42] related activities.

This document does not seek to consider factors pertaining to the events between 2020-2 in many ways, particularly with respect to the science associated with COVID & related events;

However, during the time of covid, an array of experiences were exhibited whereby persons were subject to punishment in relation to online activities, without due process. This now provides a wealth of data to assist us in defining how to deliver better digital compact outcomes.

More broadly; as is otherwise important, the underlying consideration that is considered important is the development of human dependencies upon technological systems, the

---

[38] https://www.hrw.org/news/2020/01/11/un-peacekeeping-has-sexual-abuse-problem

[39] https://www.youtube.com/watch?v=EV1NFYTwM3k

[40] https://web.archive.org/web/20150908003750/https://id2020.org/

[41] https://web.archive.org/web/20160313103740/http:/id2020summit.org/#speakers

[42] https://www.undp.org/sdg-accelerator/background-goals

uprising of AI in the public domain; and the proliferation of internet based identity and socioeconomic governance systems, at large.

Where claims of a serious nature are made on systems, particularly institutional systems; that are incorrect, (it is suggested that in many cases, statements are knowingly incorrect); there are meaningful implications, including but not limited to, consequential outcomes that will show who benefited, gainfully and who was levied the costs, as victims of conspiratorial[43] crime(s).

By seeking to establish a formal digital prison system, the ability to ensure rights for both those who are accused and/or guilty of serious crimes; becomes distinct from those who are not.

The implications now poorly considered, as inter-governmental technological platforms via united nations works, appear to have understood the importance of support for contract law, without acting upon the need to ensure 'digital wallets' support more all forms of instruments of importance, when seeking to form and execute online contracts; such as could otherwise include human rights instruments; should designs provide an inclusive approach.

should still support the means for all parties to be meaningfully supported by the tenants of historical terms; even if, the means to make such affordances are engendered by ensuring the apparatus and/or tooling provided to support e-commerce, KYC/AML, also support the means for persons to define terms in the contracts that may otherwise be applied upon them, thoughtlessly.

The Implications of AI

Artificial intelligence technology and related ecosystems are broadly - not well understood. A vast percentage of market and governance related participants, seemingly do not have an in-depth comprehension of the options, opportunities, threats and implications of choices.

Whilst some forms of AI agents have emerged and proliferated, particularly those associated with the parties most involved in the aforementioned digital identity infrastructure rollouts, yet there are other forms that can exist, that have different qualities - but are not yet available. Systems that support human rights in ways that existing systems have not shown to do…..

The construction of AI systems, is built upon the ecosystems defined to store information about agents; which includes, human beings, legal personalities (ie: incorporated entities, gov, associations, etc.) and software agents; which is in-turn built upon the definitions for how the concept of 'identity' is, by design related efforts, applied via technology systems.

"the distinction between reality and our knowledge of reality, between reality and information, cannot be made" *Anton Zeilinger*

---

[43] https://dictionary.law.com/Default.aspx?selected=310

It is considered implausible that persons are able to seek access to justice in relation to an event or circumstance for which they do not have available to them, resources stored or available in a form that can be considered evidence.

There is also the risk of records changing, or being manipulated at any stage of the life cycle; and/or, being only made selectively available and/or maintained, as a consequence of a concert of actors / agents, involved in an information lifecycle. In-order to address these issues of great importance as pre-requisites to support the intended meaning of the statements made by various values instruments, including but not limited to human rights instruments, professional codes of conduct and broadly otherwise law; the means to ensure the appropriation of technology is able to support values, is instrumental.

Should this not be the case, then arguably, there is no need for a 'digital prison', as the effect becomes that the entire environment is in-effect built as a prison, of kinds, for our thoughtware.

To avoid this dystopian future, and given the inclusion of means for people to beneficially participate in the definition of terms relating to electronic contracts as enabled by 'digital wallets'; and that the means to do so still appears to be considered, too difficult, the suggestion becomes a mandate to go about producing a formalised solution for digital prisons, as part of the broader digital social-security infrastructure sought to be produced; for all of humanity, inter-jurisdictionally.

Whilst some in the western world, may reliably or otherwise be equipped to store their own information and operate their own private & personal AI services, this is not going to be universally the case. To successfully achieve the goals outlined by UN, UNESCO, ITU, ISOC and related parties, the means to produce infrastructure where people personally depend only upon their identifiers being correctly associated with online systems in other people's computers / systems / server infrastructure; is imperatively required, to ensure support for human rights. As such, the distinction between those who are subject to punishments that are in-turn only intended to be lawfully supported subject to particular rights; and the rights of persons who are not subject to any such lawfully appropriate penalties, needs to be defined. There are so many examples of cases where people are engaged in wrong-doings in ways that employ the use of computers, connectivity and most often, economic instruments.

If the total cost upon society was measured financially & then converted to represent the volume of carbon that has been produced (ie: cost of CO2 per tonne), it is likely to be amongst the greatest of all drivers of climate change, as has been declared to be a global emergency.

It is thought reasonable to assume that veteran experts and leaders, whose works have been instrumental to the infrastructure now being deployed for digital transformation of governments, are best equipped to advance upon the requirements already established. as a consequence of their earlier 'government as a platform' works, to achieve defined SDG goals.

The foundational principles employed to define what is thought to be required, internationally, is defined by employing the UN Human Rights Instruments[44] with assumed implied parity, with respect to initial common-sense reasoning for their application with

---

[44] https://www.ohchr.org/en/instruments-listings

respect to online rights, particularly those that have a meaningful consequential impact upon persons in our world and may otherwise act to negatively impact capacity to achieve the Sustainable Development Goals..

This is a draft document provided in the interests of initiating works to deliver outcomes for the public good, given the view stated clearly that my works have never provided anything useful or helpful and that it has all been done already and that no contributions are usefully beneficial. As such; the circumstances leading to this draft document; has been brought about as a consequence of working on solutions, whereby the means to booth maintain hygiene and support rule of law, leads to an array of difficulties associated to issues that have been discussed separately in draft works seeking to define the many forms of Social Attack Vectors and in-turn, the means to address these sorts of problems by way of Safety Protocols. One of the issues identified is the need to support persons whose circumstances are believed to warrant (or as may later be found not to do so) a decision to 'exile' a user; or conversely also, the means to protect a user via systems. Which requires interoperability. As there are no clearly identifiable means to engage with systems, I started this document.

These considerations also relate to hygiene requirements for Human Centric AI works and related efforts, whereby i seek to define a particular type of implementation whilst being attentive to safety protocols. One of these safety protocols, is ensuring that there is somewhere where an offender who, associatively to consequence for wrongful actions, warrants being exiled; has somewhere that they're able to take their digital life, to maintain elsewhere.

The desirable outcome is to intentionally form a methodology to address what is required to support fairness, human rights and related considerations.

Over the past few years in particular, there have been actions taken upon persons online that have been impactful upon those who have been targeted, yet not necessarily at all reasonable.

This is considered to become part of what is essentially an underlying basis through which some form of 'digital safety net' online is considered to be required, alongside ensuring means to better address some of the - very, very serious issues and crimes that otherwise occur via ICT.

Human Rights, need to be employable online in a manner that can be used to support both

- 'web & internet prisoners' whose online use is restricted for 'fit and proper' purposes; and by extension also, the means to support probity, natural justice, procedural fairness and various other foundational principles associated to the practicalities of rule of law; AND, By extension,
- Systems would in-turn result in circumstances where any such 'prison system' is clearly distinguished from the whims of whomever may seek to threaten people or violate their rights by actions that cause harm via online infrastructure, in circumstances where no illegality exists upon a person who is otherwise more broadly, free.

Additionally; the same broad industrial areas of expertise, as employed for those who need social and law-enforcement / justice supportive 'digital transformation' related protections, may also become part of the broader requirements definition - as to support an online justice system.

In recent years particularly, it has become well known that various persons have been 'banned' or had their 'accounts' disabled, by various online services in recent times.

Some reports suggest that this has occurred in relation to foreign government policies associated with topics of public interest, welfare and the truth of the circumstances at the time, as later known.

It is also well known that there are a variety of forms of online predators, persons who are engaged in criminal and / or civil wrong-doings with the express intent to cause harm to others; in an environment where the ability to do anything meaningful about it, both to triage the threats and also, to ensure that any such practices are not gainfully employed consequently, does not have any 'good' solution to respond to these forms of challenges. Conversely, online attacks can be levied upon persons who have not engaged in wrong-doing, rather, false claims may be levied upon persons as a means to facilitate & successfully execute other wrong-doings.

It is not clear that solutions have already been defined as part of the designs formed to support global digital compact[45] and other related international works, from 2015/16[46][47] onwards.

There are also a very high proportion of online crimes without available legal remedy. The scope of implications are serious and directly associated with many serious crimes & wrongs.

Historically, society has had justice systems to support requirements. It is assumed that a more thorough illustration of the history of justice systems, is unnecessary other than to illustrate the point that the benefit of having a justice system, that includes facilities known as prisons; is that it is clearly thereafter able to be the case, that those who are not subject to any such form of sentence are therefore not otherwise required to exist within a prison.

The internet, without a prison system, gives rise to the otherwise unwanted implications of characteristics that may not act otherwise to distinguish who is indeed, upon terms consistent with law, human rights principles / instruments and related considerations subject to some form of orders; and who is not. Furthermore, much as crimes in the physical world are investigated with processes available to ensure the preservation of evidence, due-process, natural justice and various other related considerations; these too should, should continue to be supported as our documentation and evidentiary systems migrate from historic and traditional systems, to modern alternatives.

Responsibilities to Appropriate Authorities

In my works on Human Centric AI, which involves defining how to support Private & Personal AI agents, operating with particular forms of information management systems, that are required to support various functions; including but not limited to, the means to support currencies, one of the required traits is the ability to 'exile' an actor from the online platforms, that support how they are able to use their systems.
Whilst my specific designs, are coupled with an effort that seeks to ensure support for interoperability, so that no person is locked into a particular system / provider; and is able to

---

[45] https://www.un.org/techenvoy/global-digital-compact
[46] https://web.archive.org/web/20150908003750/https://id2020.org/
[47] https://docs.google.com/document/d/1GZIqlnkTzms3rIFKR18OR6VI-ksQqQGnkC5NKBgwyEw/edit

migrate between ecosystems, it nonetheless appears to be a matter of importance to ensure that there is a place for persons thought criminal, to go.

Online hosting related services, previously considered as ‘knowledge banking infrastructure’, is thought to be required in-order to support DNS (inc. domain names), back-ups, IPv6 subnets, payments / currencies, as well as various 'ai' related functions.

In developing nations, where it is not feasible to seek to ensure all individual persons / family groups; have their own equipment, there will also be a need to ensure support for services via dependency models that balance the desirable attributes to support selfhood, via electronic systems (digital transformation); and what is pragmatically able to be provided, to uplift circumstances of persons and in-turn provide foundational infrastructure that can in-turn be built upon.

Whilst these providers can be subscribed to a values based charter and various other legal instruments; and should otherwise be made able to be largely otherwise decoupled from one another, from a commercial and governance systems perspective; There still needs to be a way to act upon safety related incidents, associated to alleged serious crime.

It is also my view that the applied mechanisms should also ensure support for the means required to ensure that any false assertions end-up being both resolved, subject to compensatory measures and where appropriate, able to be employed to support further prosecutions. Some of the many Social Attack Vectors’ associate with temporal implications, that can be, via computational infrastructure, presented, should the information be stored.

Yet a problem that has existed, as does associate in-turn with the works on Safety Protocols, is about what to do with legal persons and their dependents in circumstances where claims are made that give rise to actions that may be warranted in circumstances of many serious forms of wrongs and/or crimes, but may also be injurious in cases where actions relating to deprivation and/or controls, may in-effect be found to have been applied upon the wrong parties involved.

As service providers are not law enforcement officers, juries or court judges in a court of law, and that penalties should only be applied upon others in a manner consistent with human rights principles, which is largely premised upon applied the authority of a competent tribunal and/or court of law, where the full evidence for a case may thereby be presented, considered and subsequently subject to lawful judgement; the means to support these conventions should either be supported or clearly, by well known instrument - declaratively set aside.

The idea of just deleting a persons 'digital life', modifying and/or tampering with evidence, or making it entirely inaccessible - does not support due-process requirements, and our prior inability to address these sorts of considerations is an expression of values considered to be unfortunate.

Whilst I do consider this form and/or area of deliberations about the requirements for social justice infrastructure to contain much substance associated with many difficult topics, related considerations lead to contributory foundational requirements that are thought to be important for the development of digital transformation infrastructure, as to support Human Rights & Peace.

There is an array of infrastructure requirements to support justice and Human Rights. This document is focused upon examining considerations about what is required to produce online systems that can support the digital transformation - human rights needs of persons, in circumstances where their digital freedom, liberties and/or rights are in jeopardy and/or stripped from them by other agents for the stated purpose of seeking to maintain the safety, protection and/or support of others human rights.

This document will provide considerations about the idea that it is perhaps a matter of importance to define a digital prison system, as part of the broader digital transformation agenda and its justice systems; and that this infrastructure may in-turn also support various other 'social security' related use-cases.   It is my strong view that it is not my role to engender a private force of cyber operators to police, judge and sentence users, whose lives depend upon the reliability of various characteristics of technologies that are socioeconomically instrumental.

Yet, i am equally or perhaps moreover - entirely dissatisfied with the practical illustration demonstrated historically by existing enterprise systems in the qualities that they have shown to have; with respect to their capacity to support lawfulness, human rights and various legal principles, which as an Australian - can be better demonstrated by the illustration provided by the RoboDebt Royal Commission[48] as has come about due to the actions of the same fiduciary corpus whose responsibilities have also extended to the administration of 'digital identity' infrastructure; amongst the many, broader implications overall. If it is indeed the case that they have been doing it all already, then these requirements should be easily delivered, quickly.

The Broader Lens

The implications brought about as a consequence of the production of public civil - digital identity and digital government infrastructure, is far broader than simply the issuance of identifiers.

"now is the time to renew the social contract between Governments and their people and within societies, so as to rebuild trust and embrace a comprehensive vision of human rights"

"Now is the time to end the "infodemic" plaguing our world by defending a common, empirically backed consensus around facts, science and knowledge. The "war on science" must end."

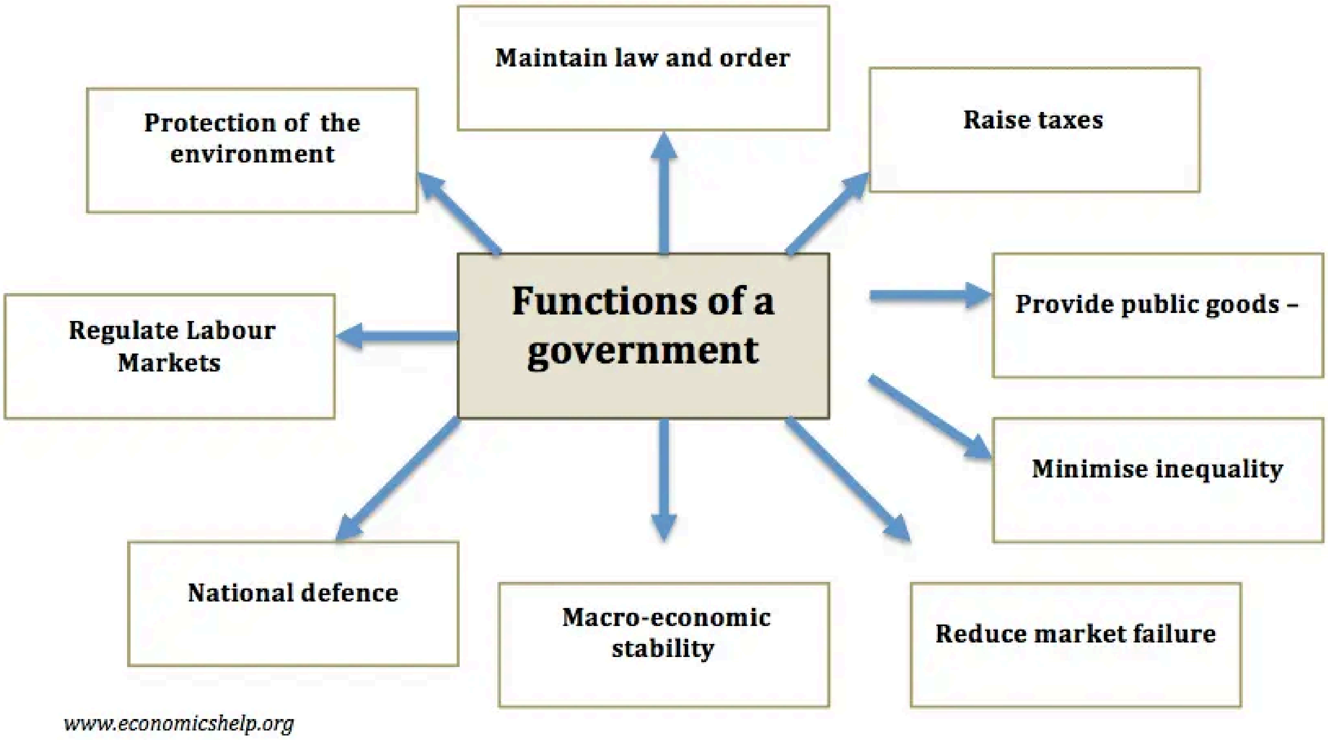
"Now is the time to correct a glaring blind spot in how we measure economic prosperity and progress. When profits come at the expense of people and our planet, we are left with an incomplete picture of the true cost of economic growth."

Source: Our Common Agenda, Report of the Secretary General, UN 2021[49].

---

[48] https://robodebt.royalcommission.gov.au/

[49] https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf



As illustrated by the above example diagram (illustratively, not specifically); There are various areas considered to be the function of government, which are of instrumental importance to the objective requirements of the digital transformation agenda requirements.

In all jurisdictions, there will be constituents who require support via the digital social security systems that have been the subject of development for some years.

It is expected that these systems internally promote their own values and laws, particularly due to the ability of governments to more easily influence the creation of legislation, as is considered to be fit for purpose by public sector workers. As such, the assumption becomes that any breaches of those values may result in the same if not greater penalties, as a consequence of any wrongs being carried out via a gainful position of public trust. Yet, in any case/event, there are still similar protections for all persons, as is important for a variety of international contexts including; investment, trade & contracts.

International Considerations

As became very clear to me during WSIS2023, there are various places around the world where the ability to ensure private market-based solutions for digital identity can be provided in a format that may otherwise be considered to be a modern capability; has a variety of forces that leads to diminished capacity, for various reasons. As such, the means to ensure some form of 'digital transformation fabric' to support the needs of all persons, requires some form of digital social security infrastructure, to support the foundational needs of those who require self-hood.

Whilst there are many considerations about 'universal basic income', some related considerations may be reasonably supported as to ensure an evaluation of what the reasonable basic attributed value for useful work should be, as may in-turn be connected to electronic evidence. This may in-turn act to promote the means through which modern forms of slavery and slavery like practices may be pragmatically addressed, as an alternative to funding 'free work', which for all intents and purposes does not exist - as is a matter of importance for SDGs.

Overall, whilst this document started by seeking to define a solution for a 'digital prison system', as a means to improve how we address issues relating to issues that invoke implications relating to some form of penalty, that may impact the ability for persons to maintain access to electronic records, systems, platforms and services; the broader considerations, results in an expansion of considerations, as manifestly influences capacity to ensure a fit for purpose justice system.

Digital Transformation

Internationally, a digital transformation agenda is well underway. The goals associated with these pursuits seek to provide support for our capacity as a human family, to deliver upon the SDGs. These requirements and related considerations associate to SDG 16[50];

PROMOTE PEACEFUL AND INCLUSIVE SOCIETIES FOR SUSTAINABLE DEVELOPMENT, PROVIDE ACCESS TO JUSTICE FOR ALL AND BUILD EFFECTIVE, ACCOUNTABLE AND INCLUSIVE INSTITUTIONS AT ALL LEVELS.

Compassion and a strong moral compass is essential to every democratic society.Yet, persecution, injustice and abuse still runs rampant and is tearing at the very fabric of civilization. We must ensure that we have strong institutions, global standards of justice, and a commitment to peace everywhere. Source: GlobalGoals.org

The implication of 'digital transformation' leads to a variety of considerations associated with the development and governance of systems, services and infrastructure; bonded to the lives of all people, directly and indirectly. The cumulative effects, leads to a dependence upon the use of systems and platforms in-order to have a material relationship with any and all rights, including but not limited to human rights, as the testament of the usefulness of rights is defined by the capacity for persons to engage in enforcement related processes, via lawfully accessible means.

Prior to broadband; laws associated to the maintenance of systems of governance, rights, responsibilities and repercussive implications were moreover dependent upon print based materials and in-turn also, communities who were engaged with one-another in a physically associative environment. Whereby, the observations of persons played an important role with law, testimony, the provision of evidence and representations provided to courts of law; online systems are different in many ways, which gives rise to the need to ensure support for values.

---

[50] https://www.globalgoals.org/goals/16-peace-justice-and-strong-institutions/

Irrespective of what is done, the derivative output becomes a representation of what values are in-fact materially supported, as may in-turn be evaluated by more sophisticated software agents. As such, the declarative means and/or practical realities of how we define values, is important in many ways; for many different types of agents, and in-turn also, the future of AI.

Life, Law & Electronic Systems

The ancient Romans formulated many laws which were applicable to all Romans, irrespective of their position.

Whilst the level of progress is different in different regions, as is in-turn the qualities of how systems are defined to operate; increasingly the records of a person's life, their actions, issues and experiences is all held online; often, on 'free' online, connected platforms. Providing the means for people to communicate with one another, which in-turn also act to store and operate their 'address books', which are no longer held by them independently but rather - governed by online platforms alongside other 'data'.

When these services are influenced by rules defined upon them, that may lead to a variety of different sorts of ramifications, irrespective of whether or not any penalty has any lawful merit; this impacts the lives of persons. In the worst case scenarios, the assessment of behaviours may lead to the person being exiled or 'banned' from the platform, which may occur without a report being made to law-enforcement officials, without means of available lawful remedy and without necessarily being associated to law or proper penalties, as would otherwise be defined in the material world.

In these types of situations; the means to maintain access to evidence relating to wrong-doing is often not able to be provided, or not able to be provided easily or in a timely or 'fair' manner.

This is particularly the case also where persons have been harmed online by other actors, who may be using pseudonyms and/or creating an array of accounts to attack target(s); whereby law enforcement recommendations range from leaving the harmful content online so that they are able to investigate (if indeed they do so, at all); to seeking the content be removed, thereby revoking the ability for the content to be available for a court of law to prosecute alleged perpetrators of crimes and/or acts of violence intended to harm, cause injury, etc.

Presently, there is a difficulty seeking to maintain support for actors engaged in meritorious behaviours, whilst forming an approach to better address the issues associated with those who are purported to have been engaged in behaviours to do otherwise.

Whilst the solutions require both social policies, investment and indeed also technological methodologies; the idea of a formal online justice system, is not considered to be something that has previously been made deployable in a 'fit for purpose' manner.

Therein, as defined by human rights statements; that even prisons have rights, the means to support proportionate penalties, as defined by a competent tribunal and/or court of law, requires infrastructure to support the means for people to be fairly treated from the time an alleged act of wrong-doing invoking a requirement to exclude a person from a platform and/or system, through to a lawful judgement; and consequentially thereafter, an environment in which a person may 'pay their debt to society'...

These considerations are in-turn summarised to require an approach for a formal technological system for furnishing an online criminal justice / prison system, to be fit for purpose.

The question of whether a person's penalty for engaging in wrong-doing should or should not be subject to the determinations of tyrannical rule, is presently unclearly resolved and/or considered. As support for human rights requires a means to ensure at all times, penalties are able to be made proportionate to the nature of alleged crimes; and that acts and circumstances of accumulative wrong-doings, victimising persons whose case may be unclear until heard by a court of law, as to determine guilt or innocence; is either sought to be endorsed or discouraged.

As engaging in wrong-doing is historically considered to be something to be discouraged; those who are otherwise innocent, should reasonably maintain restraint, even if harmed as a consequence of the behaviours of others, who have elected not to do so. Whether those who have no right to engage in wrongs, benefit & simultaneously extinguish the right for persons to seek natural justice, lawful remedy and compensation, may be a decision that remains reserved.

As such, a formal online prison system is thought to provide meaningful support to better engage with difficulties online, as the consequential issues become more easily addressed - by law, overall. Thereby ensuring that the standing of persons cannot be eradicated at the whim of another civil society person and/or actor, who is not otherwise considered a law-enforcement officer, agent, or other entity bestowed the legal right to administer prosecutorial actions upon others. Whilst more broadly considering the importance of accountability in any-case.

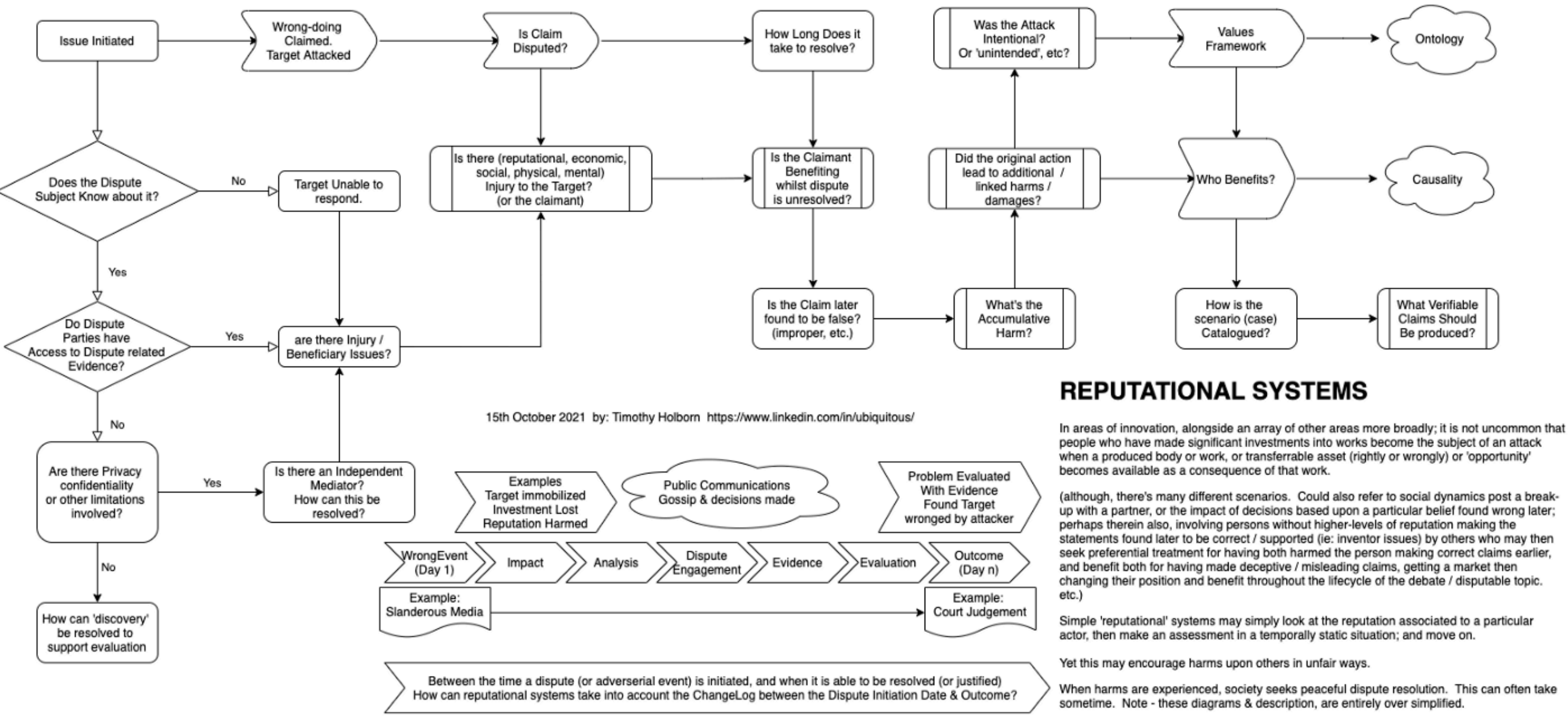
Social Protections Structural modelling.

In-order to define what functions are required for those whose circumstances and/or behaviours warrant lawful interference, restrictions, tracking, exclusions or other forms of lawful punishments; the means to define what persons should otherwise expect is made useful.

Therein, for those who are otherwise not accused of a crime awaiting and/or in the midst of legal procedures and/or those convicted of crimes, should otherwise be expected to be provided as a foundational part of being furnished the necessary apparatus to support self-hood and in-turn also, personhood, human agency, human rights?

By providing means to define a framework through which lawful punishment is provided governance apparatus and supporting infrastructure, the means to also define what rights should exist otherwise, becomes an implied series of defined characteristics, that whilst said to have been done already; i am not yet aware of how these existing frameworks are usefully employed by persons, particularly those of lesser socio-economic means and/or disability.

Justice Infrastructure: Human Rights & Rule of Law


Issue Initiated
Wrong-doing Claimed. Target Attacked
Is Claim Disputed?
How Long Does it take to resolve?
Was the Attack Intentional? Or 'unintended', etc?
Values Framework
Ontology
Does the Dispute Subject Know about it?
No
Target Unable to respond.
Is there (reputational, economic, social, physical, mental) Injury to the Target? (or the claimant)
Is the Claimant Benefiting whilst dispute is unresolved?
Did the original action lead to additional / linked harms / damages?
Who Benefits?
Causality
Yes
Do Dispute Parties have Access to Dispute related Evidence?
Yes
are there Injury / Beneficiary Issues?
Is the Claim later found to be false? (improper, etc.)
What's the Accumulative Harm?
How is the scenario (case) Catalogued?
What Verifiable Claims Should Be produced?
No
Are there Privacy confidentiality or other limitations involved?
Yes
Is there an Independent Mediator? How can this be resolved?
No
How can 'discovery' be resolved to support evaluation
Examples Target immobilized Investment Lost Reputation Harmed
Public Communications Gossip & decisions made
Problem Evaluated With Evidence Found Target wronged by attacker
WrongEvent (Day 1)
Impact
Analysis
Dispute Engagement
Evidence
Evaluation
Outcome (Day n)
Example: Slanderous Media
Example: Court Judgement

15th October 2021 by: Timothy Holborn https://www.linkedin.com/in/ubiquitous/

Between the time a dispute (or adverserial event) is initiated, and when it is able to be resolved (or justified)
How can reputational systems take into account the ChangeLog between the Dispute Initiation Date & Outcome?

REPUTATIONAL SYSTEMS

In areas of innovation, alongside an array of other areas more broadly; it is not uncommon that people who have made significant investments into works become the subject of an attack when a produced body or work, or transferrable asset (rightly or wrongly) or 'opportunity' becomes available as a consequence of that work.

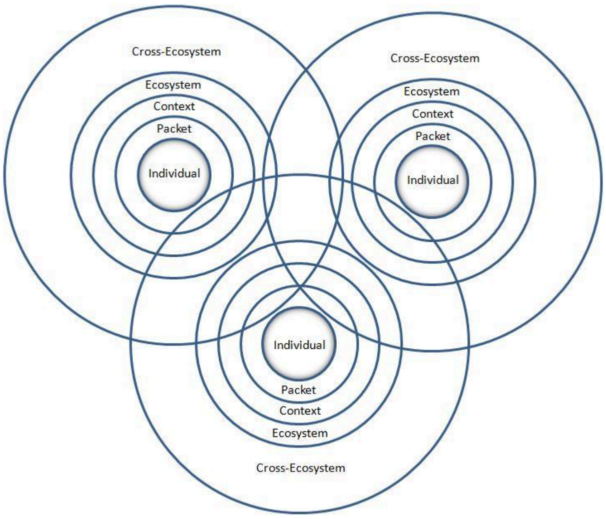
(although, there's many different scenarios. Could also refer to social dynamics post a break-up with a partner, or the impact of decisions based upon a particular belief found wrong later; perhaps therein also, involving persons without higher-levels of reputation making the statements found later to be correct / supported (ie: inventor issues) by others who may then seek preferential treatment for having both harmed the person making correct claims earlier, and benefit both for having made deceptive / misleading claims, getting a market then changing their position and benefit throughout the lifecycle of the debate / disputable topic. etc.)

Simple 'reputational' systems may simply look at the reputation associated to a particular actor, then make an assessment in a temporally static situation; and move on.

Yet this may encourage harms upon others in unfair ways.

When harms are experienced, society seeks peaceful dispute resolution. This can often take sometime. Note - these diagrams & description, are entirely over simplified.

The above diagram (seeAlso: Link to bigger image) attempts to describe the practical realities associated with resolution of disputes and in-turn procedural requirements, which does in-turn lead to considerations and implications of causal relevance and effect[51], which may impact victims in ways that may have no negative consequences upon abusers.



All circumstances of dispute start with an event that leads to one of more allegations. When unable to be addressed, the events relating to a dispute can evolve and develop into circumstances of cumulative harms, which is sometimes a strategy knowingly employed, 'to win', irrespective of reality, the truth of a circumstance; if the victim, has no access to justice or if the stakes are made too burdensome as to invalidate the concept, then certain values prevail.

Irrespective of the applied ideology about how the lens of justice be applied, there is still now therefore an invoked requirement for reasonable precautions to be made to protect the public interest, in a manner that is constituent with the ideals sought to prevail in a jurisdiction. It is not at the stage of an alleged act of wrong-doing ("claim") that judgement be reasonably available, in many cases.

---

[51] https://github.com/WebizenAI/sensedocs/blob/main/Attachments/Diagram16.jpg

As any acts considered to be a form of criminal offence or other event that may require determination and judgement by a court of law, would not have already been accomplished - at that stage.

Justice infrastructure to support these principles is of little consequence, if the ability to ensure the alleged perpetrator of a crime and/or action that invoked a reasonable basis upon which penalty may be reasonably considered in a fit and proper manner (ie: privacy considerations), becomes structurally invalidated via technology & applied policies. Yet, if the belief is that lawful judgements be applied upon persons; in a manner that is believed to be upheld following careful consideration by courts of law, who is equipped to be presented evidence in a manner that support proportionality & fairness; then the infrastructure to provide safeguards against contempt of (court/) lawful processes, is seemingly a prerequisite.

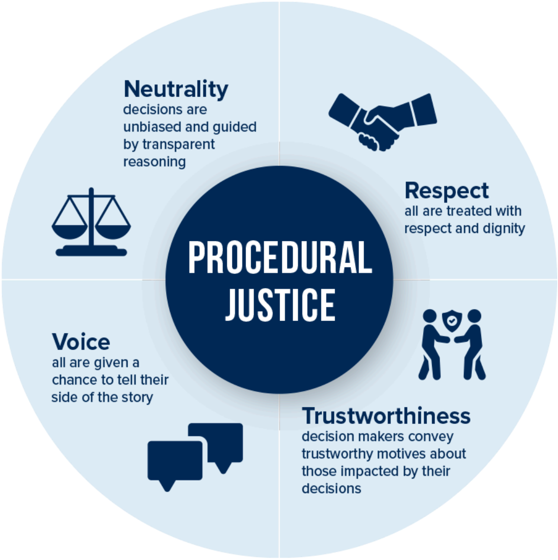

Neutrality
decisions are unbiased and guided by transparent reasoning
Respect
all are treated with respect and dignity
PROCEDURAL JUSTICE
Voice
all are given a chance to tell their side of the story
Trustworthiness
decision makers convey trustworthy motives about those impacted by their decisions

Image Source: law.yale.edu[52]

Therein, the assumption becomes - that designs should support the means to support court-related determination and/or agreement between parties, if the governance of systems is honourably intended to support correctional responses, as may be reasonably considered appropriate.

In-order to support Natural Justice, as *"the basis for the rule against bias is the need to maintain public confidence in the legal system"*[53] technological infrastructure to support the means through which cases may reach that conclusion with due-process, must be appropriately defined in such a way that does not strip evidence from the matter relating to interventional activity being applied upon a party by others. Nor unreasonably impinge upon persons rights at any time.

As is otherwise considered to be important within civilian domains, at peace or at war; particularly thereafter also, given that the digital transformation agenda inextricably requires inter-jurisdictional support, as to ensure support for the clear minded values outlined by various human rights instruments[54] alongside many other instruments and conventions, including but not limited to the salient points that still remain, from the magna carta, as was negotiated in a church in Holborn[55] and was issued in June 1215[56].

"The Magna Carta became the foundation of the idea that the king was not above the law. This has developed over time into the concept of the rule of law: the idea that all people are equal before the law."[57]

---

[52] https://law.yale.edu/justice-collaboratory/procedural-justice

[53] https://en.wikipedia.org/wiki/Natural_justice

[54] https://www.ohchr.org/en/instruments-listings

[55] https://www.londonxlondon.com/the-best-things-to-do-in-holborn/

[56] https://www.parliament.uk/about/living-heritage/evolutionofparliament/originsofparliament/birthofparliament/overview/magnacarta/

[57] http://www.magnacartalegacy.org/magnacarta.html

It is said that “Magna Carta exercised a strong influence both on the United States Constitution and on the constitutions of the various states. However, its influence was shaped by what eighteenth-century Americans believed Magna Carta to signify. Magna Carta was widely held to be the people’s reassertion of rights against an oppressive ruler, a legacy that captured American distrust of concentrated political power”[58]. These sorts of considerations thereafter lead to efforts to seek to define solutions for the web; as was the subject of a Ted Talk in 2014: Tim Berners-Lee: A Magna Carta for the web[59], and closely associated to the context of works empowered by the support of the United Nations from at least 2015 onwards[60][61].

Imagine what our world may be like, if only the king was provided the right to define the terms on the instrument now otherwise known, as the magna carta.

Whilst one might hope that support for the constituency requirements for our systems of law, it is presently not obvious that this has already been done. As such, the means to better understand the temporal factors and events[62] involved, alongside ensuring that past works are more easily identifiable is thought to be usefully helpful, as part of the process of ensuring any future efforts, best optimise the use of energy / lower the carbon foot-print, as practices that may otherwise duplicate existing works, is sought best to be avoided. Such considerations are thought to be in-line with the principles and goals outlined by the sustainable development goals, and in-turn also, the various other initiatives underway to achieve the 2030 goals overall..

Should it be found to be the case that

A. significantly more work is required to produce and/or better illustrate how prior works provide solutions for furnishing reasonable protections, to support public safety; and/or,

B. that particular forms of ecosystem constituencies do not appear to presently exist; then,

an outline of the characteristics and properties of what does exist, and what is lacking, may provide the assistance needed, to collaboratively accelerate development, build upon methods and models that may employ the language produced, at great effort in former years, as is now already embodied by the human rights instruments that are thought to provide a guiding light.

Yet, it appears to me,that the absence of means to ensure that there is infrastructure frameworks to support ‘AI / Digital Prisons’ in a manner that is distinct from the liberties otherwise sought to be afforded to all persons not suspected or accused of a crime, gives rise to legitimising concerns held by an increasing number of persons, that the entire system is in-fact designed to be the prison, with no distinction otherwise deemed necessary; nor, by implication also, support for human rights or any rights whatsoever, given the qualities of AI & ICT overall.

Assuming this is not the intent, the definitions afforded to ensure support some form of online ‘personal online data’ storage & services, as required to support an ‘Ai / ICT prison

---

[58] https://www.loc.gov/exhibits/magna-carta-muse-and-mentor/magna-carta-and-the-us-constitution.html

[59] https://www.youtube.com/watch?v=rCplocVemjo

[60] https://web.archive.org/web/20150908003750/https://id2020.org/

[61] https://web.archive.org/web/20160313103740/http:/id2020summit.org/#speakers

[62] https://timeline.knightlab.com/

facility'; to store and provide the services allowed - whilst the subject / account holder and/or 'person' is subject to correctional / legal sentencing consequences, until such a time as the matter be discharged, set aside, dispensed with and/or dismissed, should be made known or defined.

Digital Social Security

An important area of consideration that better appears to have been considered in various ways, are the requirements associated with the provision of social-services/security infrastructure.

Use-case examples include; consideration for persons,

- *Who has died or is declared missing.*
- *Require Emergency Intervention.*
- *Are Subject to Criminal Cyber-Attacks.*

Known to be suffering from,

- *Poverty.*
- *Domestic and/of Family Violence.*
- *Acute mental illness of a kind, such as psychosis or similar, leading to safety concerns.*

Special Needs,

- *Protected Persons*
- *Politically Exposed Persons.*
- *Legal Aliens*
- *Refugees*

Non-Natural Persons (legal personhood, other than for natural persons)

- *Entities and/or the information pertaining to Events associated to legal deliberations*
- *Software and systems requiring intervention and/or protection of some form.*

Imagine, if a person was being attacked online, and there was a button that they could press that provided the information associated with the incident to a secure platform, for protection, review and the means to seek help for personal safety.

Online systems often seek monthly charges, and not all are able to afford these fees and/or rents. So, the question becomes - how could these sorts of infrastructure services also provide broader social-security & safety-net features, for those who are unable to employ market-based alternatives.

Therein also, the means for persons who are subjected to crimes as victims (victims of crime); and indeed also, refugees and other persons whose needs are particular, including but not limited to those involved with secrecy and/or public service, such as law enforcement, politically exposed persons, those whose circumstances are managed by state trustee / guardianship services; and a variety of other categories overall.

Technical Solutions: Standards - Past, Present & Emerging

Presently, the primary solution provided by the major platforms is the ability to 'download your data' as was advanced in 2018[63] with the Data Transfer Project[64]. However, there are many characteristics of these solutions that are thought to be lacking, in-terms of broader 'fit for purpose' requirements and related considerations.

The material implied requirements are not simply served by being able to 'download' a person's information; rather, the electronic information needs to remain functionally employable and able to be restored. As such, the technical challenge is in defining how to provide and support safety requirements for these cases. It is thought often to be the case that the means to communicate and retain & maintain records; for legal and various other human rights purposes, as well as many other good reasons, is considered to be a vital requirement for law.

However, the construct of how to define appropriate terms in an interoperable manner internationally, would appear to be one of the many more significant challenges, if indeed this infrastructure is not already in place. As such, it is thought that modern solutions need to be defined as to support human rights requirements as may be considered by reviewing the texts of the instruments produced via the quorum of the United Nations[65] as well as others, overall.

The means to ensure systems are still able to be considered 'evidentiary' (tamper evident); as well as continuing to be functionally useful (ie: address-book / contact lists, etc) are amongst the qualities that are not easily shown to apply to these existing online offerings.

The broader implication becomes a requirement for online platforms to ensure that users are able to be migrated to these systems that provide digital justice and social security services. in-turn also leading to considerations about how various emerging requirements will interact with the broader needs of furnishing a fit for purpose social safety net - online with AI.

Solid

Whilst there are many complex reasons why my considerations lead me to put forward the fairly specific idea of delegating the problem to the leaders of the W3C works known as Solid, as led by Tim Berners-Lee. Noting the video "the Global Digital Compact produced by World Wide Web Foundation and partners"[66], as is amongst the notes provided about the global digital compact[67].

The World Wide Web Foundation was established in 2009 by web inventor Sir Tim Berners-Lee and Rosemary Leith to advance the open web as a public good and a basic right. Best known as the inventor of the World Wide Web[68]; In terms of how to define a web-solution, there are few more qualified. In 2018, Berners-Lee took a sabbatical from MIT to launch a commercial venture based on Solid, named Inrupt[69].

---

[63] https://techcrunch.com/2018/07/20/data-transfer-project/

[64] https://datatransferproject.dev/

[65] https://www.ohchr.org/en/instruments-listings

[66] https://www.youtube.com/watch?v=TeqbLksgcGE

[67] https://www.un.org/techenvoy/global-digital-compact

[68] https://en.wikipedia.org/wiki/Tim_Berners-Lee

[69] https://en.wikipedia.org/wiki/Solid_(web_decentralization_project)

It appears that the ideological manifestations, requirements, designs and characteristics of 'solid', make it an competitive choice when seeking to identify a possible solution to achieve these goals. Solid, as led by inrupt, has already demonstrated its capacity[70] to provide user 'pods' to store their personal information, in a manner that has been declared to support AI services[71] and various other related characteristics. Solid works, are developing a W3C standardisation effort[72]; as such, should offer the means to provide a set of standards that can be supported by various platforms as a future 'web standard'. Solid provides a potential technical solution to ensure that when actions are taken upon persons, rightly or wrongly, as to be defined by a court of law, even if only made available long-after online penalties; that the means to retain evidence of the circumstances, and support for the human rights of the parties involved, whilst seeking lawful remedy, justice and/or compensation, can be maintained.

The effect of 'fit for purpose' justice infrastructure may well result in disruptive influences, as accusers end-up being found to have been perpetrator, rather than victims or rescuers; the consequence of not having a solution to address these problems, is tyrannical, and fundamentally aligned with the interests of those most adapt at gainfully engaging in organised crime; as is influenced by the circumstances of how systems work as to support law or by design, designs that seek to set such forms of human rights related considerations aside.

Evidence Standards

ISO/IEC 27037: Security techniques, Guidelines for identification, collection, acquisition and preservation of digital evidence. This standard concerns the initial capturing of digital evidence.

ISO/IEC 27041 offers guidance on the assurance aspects of digital forensics e.g. ensuring that the appropriate methods and tools are used properly.

ISO/IEC 27042 covers what happens after digital evidence has been collected i.e. its analysis and interpretation.

ISO/IEC 27043 covers the broader incident investigation activities, within which forensics usually occur.

ISO/IEC 27050 (in 4 parts) concerns electronic discovery which is pretty much what the other standards cover.

British Standard BS 10008:2008 "Evidential weight and legal admissibility of electronic information. Specification." may also be of interest.

Source: iso27001security.com

Note also: https://en.wikipedia.org/wiki/Chain_of_custody

---

[70] https://www.inrupt.com/blog/digital-flanders-reconnects-citizens-with-their-data-through-inrupts-solid-server

[71] https://www.cnbc.com/beyond-the-valley-podcast/

[72] https://lists.w3.org/Archives/Public/public-solid/2022Nov/0001.html

Formalisation of Cyber Justice Infrastructure.

In recent times, it has become commonly known that persons have been sent to 'social media prison', having their accounts terminated and/or revoked; in some cases, for ever, in other cases, for a period of time until a change of management shifted the policies & reinstated users accounts.

These sorts of actions have had a significant impact upon society as a whole, as well as the people who were directly subjected to the consequences of actions by platforms. It is believed that in many cases the persons disaffected did not act unlawfully, and reports since, suggest targeting was involved. Part of the implication of these sorts of actions also leads to on-going problems, as algorithms and systems generate and store information to decide how voices are prioritised.

Yet, conversely, serious crimes that occur via online systems, such as spam, fraud, money laundering and various other forms of cyber-crime; as well as the on-going issues relating to child-exploitation and human trafficking, for some reason appear to be an on-going problem.

In-order to define what are the sorts of characteristics that should be associated with the concept of a form of lawfully appropriate punishment, the ability to define both; what the functional qualities of a digital prison system should functionally require; whilst also invoking means to better illustrate the sorts of digital rights should otherwise be available for all others, and in-turn also, the means to ensure that those who have been falsely and/or wrongly targeted, have rights as would otherwise be the case if they were subjected to harms by any other agent.

By ensuring the Digital Transformation Agenda takes into consideration the requirements to support rule of law, human rights and various related responsibilities, the objective benefit should be the creation of solutions to successfully prosecute persons engaged in serious crimes.

Notes from Chat GPT

Asking ChatGPT to provide some history, has resulted in the following information being provided per below; the accuracy of the information provided, is unknown. It is also important to note that there are various Ai related use-cases that presently appear to lack means to better consider how the rules should be applied in a people centred internet to all forms of 'people', and indeed also - how different definitions for different words exist, in different jurisdictions...

In any event the feedback provided so far by ChatGPT about the history of 'digital prisons'; is as follows,

The history of online penalties applied to persons and/or user accounts is relatively brief but has developed significantly in recent years.

Here are some key milestones:

1. *Terms of Service (ToS) Agreements: Early online services, such as CompuServe and Prodigy, established terms of service agreements in the 1980s and 1990s to set rules for user behaviour. Violating these rules could result in account termination.*
2. *Digital Millennium Copyright Act (DMCA): The DMCA was enacted in 1998 in the United States to criminalise the production and dissemination of technology that could circumvent measures used to protect copyrighted works. It also provided penalties for online copyright infringement.*
3. *Cybercrime Conventions: International conventions, such as the Council of Europe's Convention on Cybercrime, were developed in the 2000s to harmonise cybercrime laws and increase cooperation between countries.*
4. *Social Media Policies: As social media platforms became more popular, they developed their own community guidelines and policies to regulate user behaviour. Violating these policies can result in penalties, such as content removal, account suspension, or even permanent account termination.*
5. *Online Harassment and Hate Speech Laws: In recent years, many countries have enacted laws specifically targeting online harassment and hate speech. These laws aim to hold individuals accountable for their actions online and provide penalties for behaviour that violates the law.*
6. *Digital Prisons: The concept of digital prisons, or virtual correctional facilities, has been proposed as a potential solution for cybercrime. This would involve incarcerating offenders in a digital environment rather than in physical prisons.*

Overall, online penalties have evolved in response to the changing landscape of the internet and the need to regulate user behaviour. As the digital justice system continues to develop, it is likely that we will see further changes in how penalties are applied online.

The concept of digital prisons, or virtual correctional facilities, is a relatively new idea and has not yet been fully implemented. However, there are some examples of digital prisons being explored or used in various parts of the world:

1. *Estonia's Digital Rehabilitation Program: Estonia has been exploring the use of digital rehabilitation programs for offenders since 2016. The program uses a virtual environment to simulate real-world scenarios that offenders may encounter when they are released from prison. The goal is to provide offenders with the skills they need to reintegrate into society and reduce recidivism rates.*
2. *Norway's Online Prison: In 2014, Norway opened a digital prison where low-risk offenders can serve their sentences from home. Offenders wear electronic tags and are monitored by a control centre that can track their movements and ensure they are complying with the terms of their sentence.*
3. *China's Internet Addiction Treatment Centers: China has several internet addiction treatment centres that are designed to help individuals who are addicted to online gaming or social media. The centres use a combination of therapy and digital detox programs to help individuals overcome their addiction.*

4. *Virtual Reality Correctional Training: In the United States, some correctional facilities are exploring the use of virtual reality training programs to help prepare officers for real-world scenarios. The programs simulate situations that officers may encounter, such as riots or hostage situations, and provide them with the skills they need to respond effectively.*

It is important to note that the concept of digital prisons is still in its early stages, and there are many potential ethical and legal implications that need to be considered before it can be fully implemented.

There have been many examples where social media platforms, search engines, and operating systems have removed content or applied penalties to users for violating their policies.

Here are some examples:

1. *Social Media Platforms: Social media platforms like Facebook, Twitter, and YouTube have all removed content or applied penalties to users for violating their community guidelines. For example, in January 2021, Twitter permanently suspended former US President Donald Trump's account due to repeated violations of their policies.*
2. *Search Engines: Search engines like Google have also applied penalties to websites for violating their policies. In 2020, Google removed 2.7 billion "bad ads" and suspended or terminated 1.3 billion accounts for policy violations.*
3. *Operating Systems: Operating systems like Microsoft have also taken action against users for violating their policies. In 2020, Microsoft announced that they had removed over 100,000 malicious and misleading apps from their app store and had terminated thousands of developer accounts for violating their policies.*

It's worth noting that the policies and penalties applied by these platforms can vary depending on the specific platform and the nature of the violation. Some violations may result in content removal, while others may result in account suspension or termination. Additionally, there is often debate and criticism about the enforcement of these policies, as some argue that they may infringe on free speech rights or be applied inconsistently.

Post-GPT - Input related Considerations

Whilst the above information only provides a relatively simple introductory summary, it might be noted that the relationship between online penalties and law; is not thought to be very well aligned.

Human Beings, can in-effect be punished for activities that relate to truth-telling, which particularly disaffects persons who engage in doing so in the early-stages of a topics events and public discussions; which in-turn acts to perform a form of ideologically defined applied socioeconomic & reputational investment structure, that may not in-fact be lawful.

In-order to support #RealityCheckTech as is required to support human rights & SDG16, the systems that are implemented to advance progress of the digital transformation agenda, should seemingly also consider the importance of ensuring that technology supports the values defined by human rights instruments; including but not limited to those defined by the Universal Declaration of Human Rights[73] (see XML versions[74])

Whilst the legal notion of ‘person’ varies by jurisdiction, it is thought that many of the American interpretations of the concept of person or personhood, refers both to natural persons, legal personalities (ie: companies /corporations) and more recently also, software systems[75].

In consideration of the people centric internet[76] works now endorsed by many involved in the international activities to support the digital transformation agenda, with the UN, ITU, WHO, ISOC and various other stakeholders, whilst noting human centric alternative views, support for jurisdictions is an important part of the international infrastructure requirements.

As the use of technology is linked with ‘choice of law’ provisions, associated to contract, intellectual property and trade law related systems; now therefore, as is associate to the legal interpretations of language associated to ‘choice of law’, as elected by platforms, an engender interpretation of the term legal persons alongside ‘legal aliens’; impacts,

- How rights are afforded, may reasonably be sought to be made clear for all contracting parties & thereby also;
- Internationally supported, As to make clear, who may be presumed to be associated to the rights, privileges and responsibilities of law, in an equitably associative manner as is otherwise the case for human / natural persons,

  whose *inalienable* human rights are now so very much influenced by these other forms of agents and/or ‘people’, seemingly empowered to govern their own private justice system.

In-order to define how UN Instruments should be applied to support the rights of prisoners, the means to define how the same instruments should be applied to support us all, is required.

Support for Separation of Powers

Separation of powers refers to the division of a state's government into "branches", each with separate, independent powers and responsibilities, so that the powers of one branch are not in conflict with those of the other branches. The typical division into **three branches of government**, sometimes called the ***trias politica*** model, includes a legislature, an executive, and a judiciary. Source: wikipedia[77]

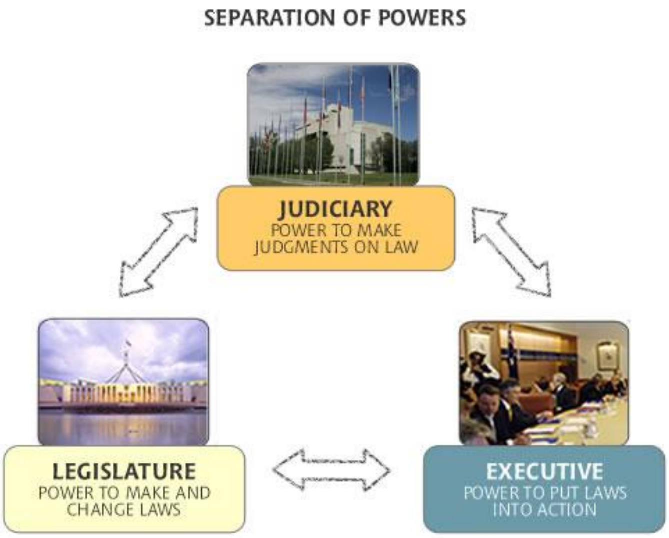
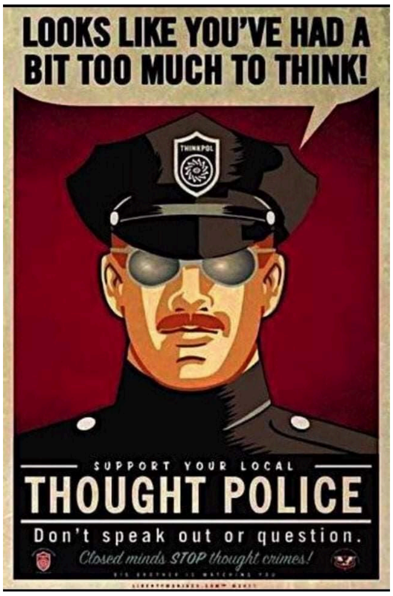

SEPARATION OF POWERS
JUDICIARY
POWER TO MAKE JUDGMENTS ON LAW
LEGISLATURE
POWER TO MAKE AND CHANGE LAWS
EXECUTIVE
POWER TO PUT LAWS INTO ACTION

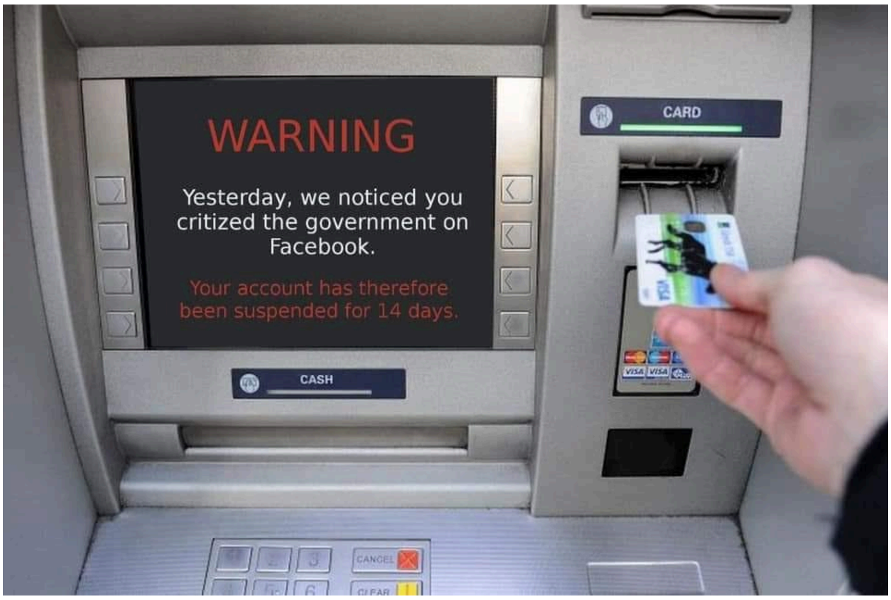
Image Source: peopleint.wordpress.com

---

[73] https://www.un.org/en/about-us/universal-declaration-of-human-rights
[74] https://github.com/unicode-org/udhr/tree/main/data/udhr
[75] https://www.forbes.com/sites/digital-assets/2023/03/07/-new-hampshire-utah-recognize-daos-as-legal-persons/?sh=7ab80be6586b
[76] https://peoplecentered.net/
[77] https://en.wikipedia.org/wiki/Separation_of_powers

This & other types of systems do not necessarily support human rights when associated with international online systems, platforms and related associative considerations. Whether made a requirement or a choice, if people are subject to actions that infer wrong-doing, they should be able to opt to migrate their accounts elsewhere, if not required & able to opt to be only lawfully punishable subject to the terms, processes, requirements and responsibilities defined by law.


LOOKS LIKE YOU'VE HAD A BIT TOO MUCH TO THINK!
THINKPOL
SUPPORT YOUR LOCAL
THOUGHT POLICE
Don't speak out or question.
Closed minds STOP thought crimes!


WARNING

Yesterday, we noticed you critized the government on Facebook.

Your account has therefore been suspended for 14 days.

Associative Analysis of UN Instruments for Online Systems

There Are many who have significant concerns about the implications of what the digital transformation agenda will have upon the lives of persons. In consideration, the means to clearly define rules both for persons who are not subject to lawful investigation and in-turn also those who are; are thought best considered, in the first instance, via the lens of how the employment of Human Rights Instruments for Digital Transformation related needs, may usefully support a foundational lens that may assist ecosystems stakeholders to illustrate how existing systems are already ‘fit for purpose’ and/or means to define, what needs to be achieved.

(Work in progress)

https://docs.google.com/spreadsheets/d/17WfvOyoVQDv8wwPYroX6xrKLM7n3stD9vFv4rejqmo8/edit?

The United Nations Standard Minimum Rules for the Treatment of Prisoners

https://drive.google.com/file/d/1wewhRd04iRkhx13C7szWwDyz_5Spyt4f/view?usp=sharing

Anti-Human Trafficking Manual for Criminal Justice Practitioners

https://www.unodc.org/unodc/en/human-trafficking/2009/anti-human-trafficking-manual.html

https://www.ohchr.org/en/special-procedures/sr-slavery

https://unglobalcompact.org.au/business-human-rights/modern-slavery/

https://www.ohchr.org/en/stories/2021/07/moderating-online-content-fighting-harm-or-silencing-dissent https://www.ohchr.org/en/business-and-human-rights/b-tech-project

https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression

Resource Notes

https://www.unsw.edu.au/news/2021/02/new-online-safety-bill-could-allow-censorship-of-anyone-who-enga

https://enlighten.griffith.edu.au/the-ethics-of-cancel-culture/

https://theconversation.com/deplatforming-online-extremists-reduces-their-followers-but-theres-a-price-188674

Further Reading

(Work in progress)

Note; as part of the broader ‘peace infrastructure project’ library,

https://drive.google.com/drive/folders/1tYFIggw8MIY5fD2u-nbwFRM6wqrhdmQZ

There is a section on technology and ethics,

https://drive.google.com/drive/folders/1uwGax8GvZA2jzJ_UFIoYppijZX4vDsoL

Gov & defence (particularly therein - note cyber)

https://drive.google.com/drive/folders/1RzE_QQbBRyE0druVpvffQoT5KDms_5mT

Other Related Links

https://www.un.org/techenvoy/global-digital-compact

https://sdg.iisd.org/events/summit-of-the-future/

https://www.govstack.global/

https://aiforgood.itu.int/

https://dial.global/

https://giga.global/

https://projectconnect.unicef.org/map

Social Security systems

https://github.com/openimis

Digital Public Goods: https://digitalpublicgoods.net/

TODO: Lots.

Also, make a list of all the available ‘digital identity’ videos that are available online. Create a table of all the features / functions that each of them now appears to provide…

Update / improve timeline of ‘digital identity’ stuff.

https://cdn.knightlab.com/libs/timeline3/latest/embed/index.html?source=1Kab5bDqGkCGwkOUlAQ8NNlNUUBBVyzXQaYS9q6jLDZo&font=Default&lang=en&hash_bookmark=true&initial_zoom=3&height=900#event-digital-id-the-ssi-story-etal

Produce insights / information about the impact ecosystems will have, incorporating IoT, etc.

Add Additional Projects related to the broader ecosystem goals.

Considerations about providing minimum requirements to support learning & safety

https://docs.google.com/document/d/1D63FlICIOXcnLx_PYs0ByLYvc1B-BXqhhXGdaW_rIMI/edit

Incorporate useful parts from the following old/historical documents:

- https://docs.google.com/document/d/1aVdtsaoRUFkSviSoF64PJ4AocQoM6YjyctnnzOkhEbY/edit#heading=h.6p83yy13t1at
- https://docs.google.com/document/d/1IgqZYO4v7QU_X6Jn5Vzx2QRditmHNg2aCgU5DJ8x8mI/edit
- https://docs.google.com/document/d/14kWJhmbHKxaS0uPLiUaN5zG8MZPcKUosj--WBSBbP5U/edit#heading=h.rioj51l9lzk2
- https://docs.google.com/document/d/1I9XCBlpJ9PSOjWnhRbetBHGfWvVkik6CCIQRg76-sKo/edit
- https://docs.google.com/document/d/1IgqZYO4v7QU_X6Jn5Vzx2QRditmHNg2aCgU5DJ8x8mI/edit
- https://docs.google.com/document/d/1aVdtsaoRUFkSviSoF64PJ4AocQoM6YjyctnnzOkhEbY/edit#heading=h.6p83yy13t1at

Related Works

The information provided below, is extracted from prior works, and has not yet been edited.

Codename:Safe t(ech) net

Originally produced 22.08.2022, with input provided by now deceased Pip van Wanrooij, who had provided support for various project works seeking to improve cyber-security capabilities, since 2019.

Overview

An incident has occurred - that I have been made aware of - which I find to be horrific. The means to employ technology to address the underlying problem - today - seems too hard. Lets sort those problems out; so that people - can expect that it's safe to go to work to provide for their children.

There are an array of different types of retail businesses where there's a high-risk potential of workers being subjected to assault (assault in terms of ? - physical/digital/mental/ threats, social engineering/manipulation of data, statistical manipulation.).

These businesses are not necessarily run by wealthy persons / owners, indeed often those who work to support their families in vulnerable circumstances are amongst the persons most-likely to be targeted by criminal acts of violence.

Whilst this is not the only characterisation of vulnerability, there is a lack of means, literacy, competence, situational awareness, to protect persons engaged in particular activity types - from unnecessary harms.

In larger businesses, with a greater amount of foot-fall traffic, solutions such as ID scanners,CCTV & security are encouraged - often by law. Solutions exist for those industries, yet, it appears the same cannot be said to protect low-paid vulnerable workers.

The objective is to address these problems in a manner that addresses problems, without causing unnecessary 'unintended consequences'. (examples being… and why it matters)

Goals

The high-level goals i've considered now - whilst putting this document together are as follows;

1. To define a solution to protect workers in particular types of retail environments, both adults and children.

2. To define a solution to protect particular types of workers whose activities are on-site at other (ie: clients nominated) premises.

3. To ensure the security solution does not unnecessarily expose persons to other risks; such as identity fraud, breach of privacy, torts, financial crimes, extortion, etc.

4. To seek to ensure the economic model for providing these solutions is accessible; and that consideration be made about the cost/benefit of preventing crimes that result in significant socioeconomic costs.

5. To ensure the 'data governance' solution is governed under local jurisdiction.

As work commences to further these ideas into action - it is without question, considerations will grow.

High level Design Concept - Considerations

The principal concept is that there's an ecosystem of parts that can be set-up to create customisable solutions that act to provide safety for workers in different circumstances. (bio, economic, reputational, life events, social equity, digital...)

This design process requires an array of design specifications; that address various concerns linked with different agents involved in the ecosystem.

The belief is that this process will likely result in an innovation process, whilst forming a regulatory framework that can better clarify the rights & responsibilities of surveillance technology for use by persons who have a reasonable need to use them to be safe. (one better than we currently have available and rely upon)

Legislatively regulated use

Generally people have a right to privacy, (yes, but is this our current reality? Nope) but this does not transcend the right of others, to safety, (personal/physical/digital/bio/future self security - defined as?) freedom from violence and right to lawful remedy / prosecution of criminal abusers.

The focus of the considerations made in this document - is about ensuring safety of persons, rather than a focus on the protection of property. Part of the underlying requirement will be to ensure persons have a right to safety; both from abuse & from false claims of abuse.

Therefore; the data-collection (inc. biometrics, etc.) requirements result in a design paradigm whereby there is a desire to securely collect evidence in a manner that protects vulnerable persons. (controls of data harvesting without inherent knowledge by individuals, legal guardian)

BY DESIGN - This capacity may be initiated by any person in the environment; consumer or worker.

These considerations then lead to various broader considerations relating to the use of surveillance or recording devices in private and/or commercial spaces (as is distinct to public areas) as should carry various legal considerations. (Think police recording body cameras, woolworths, airbnb, taxis, driver training etc) If these considerations are not properly considered, the results may in-turn have the effect of negating the ability to use evidence of wrongs in a court of law to secure prosecutions. (not an expert in this area, IDK. Does it? We have advanced tech - not put to good use.)

Furthermore these systems should be designed to improve the quality of life of VIPs / PEPs, etc.

Regulatory Levels of Safety?

A concept considered is whether there may be different ‘levels’ of regulated right to use safety equipment; and that, depending on the type of application different rules apply.

Medical & Personal Services Businesses, cleaning businesses, disability support services, delivery drivers, social workers, short-term shared accommodation / backpackers, services involving children or activities that have a significant impact upon the lives of children; and that, depending on the type of application, different rules apply.

For example (intended to be illustrative - not otherwise)

I. Level 1

An optional ability to have a system in place that can be activated when required and a definition of what constituencies need to be provided as part of that defined optional requirement, etc.

II. Level 2

A requirement to have a system in place that can be activated when required and a definition of what constituencies need to be provided as part of those defined requirements, etc.

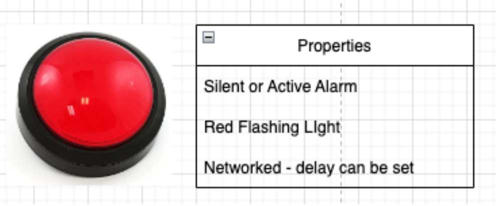
III. Level 3

A requirement to have a system in place that is ‘always on’, with an escalation capability and a definition of what constituencies need to be provided as part of those defined requirements, etc.

Technology ecosystem requirements

Visible Alarm Buttons

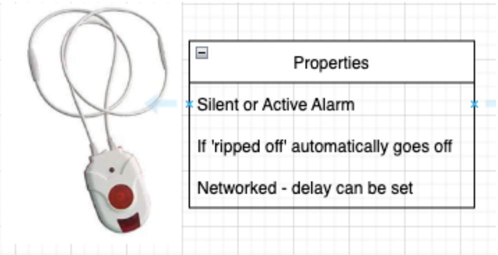
The Visible Alarm Button would flash & have a specified meaning - much like a fire safety device where, if it's on - the well known meaning is - stop what you’re doing & leave the building.



The device should be programmable in how it is set-up to operate. Some may be able to be cancelled by pressing it again in a certain period of time, other installations may require it to be cancelled via an external process in another device located elsewhere. The button may also be defined to indicate other surveillance equipment is turned on.

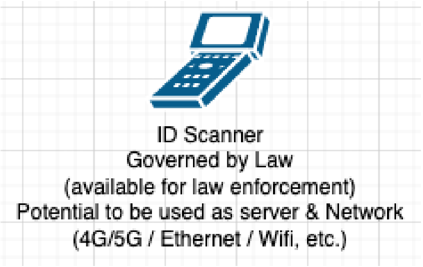
Safety Pendant

An array of safety pendants, that are connected to the network and able to be programmed to turn on either audible alarms or silent alarms or both; either, via pressing / holding buttons on the device - or in situations where it appears the device has been ripped off the person.


Properties
Silent or Active Alarm
If 'ripped off' automatically goes off
Networked - delay can be set

- A delay should be programmable depending on the situation.
- An indicator should show if it is not connected to the network, and ideally also they can be recharged.
- These devices should also be made to work with a worker's mobile phone with a specified app - if their type of work means they're working on-site / mobile…
- Be able to be integrated into an 'identity' or 'visitor' tag - associated with the person.

Regulated ID Scanner (& security server)


ID Scanner
Governed by Law
(available for law enforcement)
Potential to be used as server & Network
(4G/5G / Ethernet / Wifi, etc.)

A regulated ID scanner requires an array of markings that provides confidence to consumers that they're authorised equipment. In smaller (retail) businesses, they may also be the best way to host the software that operates the broader security environment; as a regulated device - much like EFTPOS for banking. Therein, the ability to Connect to an external network and operate a local WiFi network for security purposes - is part of what these devices should do. The underlying software used to scan identity documents should be protected from misuse - by the user (the business); although, there could be approved extensions that support the use of loyalty cards & other - non-protected forms of 'identity instruments', and the device may also connect with a Point of Sale System or similar. The expectation is that the user of this system would check the customer in / out; and that, any security related problem that may occur - triggering an alarm (by customer or worker) is then made available to an authorised provider who is able to provide reports to courts, law enforcement or other authorised recipient of the recordings, and related information.

The system could also be set-up to record network card addresses (WiFi / Bluetooth, etc.) of connected devices, alongside other programmable systems to support incident reports.

A/V Capture Devices

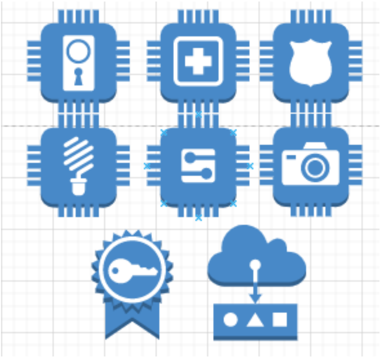
A/V (& IR) Camera
WITH VISIBLE INDICATOR

A/V Capture devices are intended to be networkable. There are specifications that should be defined - including, based on regulation - the ability to be able to visually affirm whether or not the device is on; subject to regulatory requirements / considerations, acknowledging some circumstances may allow for silent operation when it is reasonably understood that this would be entirely inappropriate in other circumstances.

These devices should act with the network to send the information to the regulated surveillance device which in-turn securely transmits the information to a regulated online service, for secure storage (and availability for use) for a specified period of time / purpose.

Automation Systems

So, using IoT related systems, there's a lot of programmable solutions that can be networked into systems that are actuated as a consequence of security related protocols. Whilst these systems may be highly customised to the environment; and not all components of these systems feature the same sorts of - problems / concerns, as to lend support for the considerations / notes about the need for some sort of regulation about how 'smart systems' can be used for safety purposes - its just worth noting - that a smart agent, may be made able to do many, many things - depending on the rules / situation.



Similarly; there's also means to assert 'rules' via the security / safety regulatory frameworks, that may also require express permission should one party require or seek personal and/or confidential information / identifiers (and linked 'graphs') on a basis that is not expressly permitted / required.

Therefore - providing a means to create a regulation framework for AR Environments, that may trigger off various types of considerations and/or rules; that may be designed to generate alerts in ways that take into consideration knowledge that not all persons associated with systems necessarily be made aware of; as to both, provide mechanisms around security / safety, alongside privacy / human dignity.

Yet - these sorts of more advanced considerations - end-up, with a whole bunch of detail related issues of great / immense importance - there are many ways 'good ideas' can be perverted to do the opposite.

Regulation - Design considerations

If these sorts of things are done 'well' (rather than 'ad-hoc') - there's an array of underlying considerations that can be employed to address various underlying matters of importance.

IV. Identity fraud

There are ways to verify whether the identifiers provide an ability to identify the person sufficiently. These capabilities have various privacy implications. Whilst a waiver may be suggested to be provided via a notice of some form; this doesn't necessarily mean that there is no-risk associated with bad-actors using ID tech kit.

V. Symmetry of rights

As much as these systems may be used to protect workers, the same principles apply to consumers. Systems should be designed to provide protection to both.

VI. Standardised Alarm & Alert Signals

There's standard signals used for emergency services, fire systems etc. It would be beneficial to produce a similar system of alerts / alarms - that are protected via regulation for use in only certain circumstances linked to specified meanings.

These considerations can in-turn be linked to public awareness campaigns that provide means for members of the public to understand what the alert means, and in-turn - be provided education about what it is they might be able to do about it.

Technology in various fields has now advanced substantially. Visual Alerts can employ LED systems - that provides a capacity to make use of different colours, in a way that was not possible for system designers to consider a decade or more ago.

Similarly, Audio systems are programmable in various ways; and in some cases, there's an ability to generate automation responses throughout buildings, etc.

VII. Electronic Recordings & Rules

There's an ability to create a regulatory environment that is able to address a balance between the needs of people - who when attacked, should not be expected to be prepared prior to the events happening; the means to discourage attacks, means to rapidly end attacks / escalate the circumstance of an attack; and the ability to have evidence relating to an attack, that can provide access to justice without expense (ie: so that justice is available for persons even if they're poor / homeless).

Therefore some consideration should be made about what the relevant levels of 'proper safety measures' could or should be; and how they associate with,

- means to ensure persons are safe as a consequence of the events relating to the use of these tools; and,
- What precautions should be reasonably provided to workers by law; and,
- What precautions should be required by law; and,

- What, by law, should not be done; and what penalties apply / how they are made enforceable.

VIII. Jurisdiction - Knowledge Management

The electronic information being collected by these systems should have rules about where and how they are allowed to be employed, stored, transmitted, etc.

The optimal case for high-stakes information should consider support for local jurisdiction (ie: if in QLD, stored in high-security data-centre / systems (ie: T3 from memory)); and that software / network operators are required to maintain security clearances / checks, etc.) The underlying systems can become highly sophisticated.

Innovation - Design Requirement considerations

It appears there isn't presently appropriate regulatory frameworks in place to do a good job at this. In-turn, there's no appropriate 'turn-key' solutions - although, they can be made; but without proper governance frameworks around it, the consequences may have an array of unintended consequences that act to undermine the intended purpose of work.

IX. Technology Innovation

There's a bunch of work that may need to be done to produce an ecosystem of parts that can be easily obtained / manufactured - to provide a 'fit for purpose' solution. However, part of these considerations also link to deliberations, about whether and/or how regulatory frameworks might require good technology - to have particular characteristics that may not presently exist - on standard retail devices.

X. Governance Innovation

There needs to be consideration about how to build / operate / support - advanced 'security fabric' systems - in a way that's accessible / affordable, has an array of functionality that doesn't act to disadvantage / harm - persons behaving lawfully (or support entrapment, etc); and that, there been a series of standards & linked vocabulary / knowledge systems - associated to how any such thing is delivered.

XI. Regulatory Innovation

There needs to be regulation frameworks to ensure the solutions that are delivered, are done so in a way that conforms to regulatory requirements - in a manner that is 'fit for purpose' and well considered overall. This will in-turn also support the means to ensure systems are used assistive to support rule of law & through that, human dignity; rather than the opposite.

Business Case

The business case(s) are built upon the means to support assurance for vulnerable persons that if they're in a vulnerable situation, where they seek to be safe and/or engage on a basis that they will not be assaulted or have their lives or those of their loved ones assaulted; that we define technology solutions to ensure we are able to address these problems in a manner that is able to be done locally, in the interests of protecting people.

The consequence of doing so will result in cost-savings & support for intervention earlier than would otherwise be possible, for persons whose behaviour needs to be lawfully addressed by law-enforcement and/or mental health facilities and/or both.

It is desirable that business systems be forged in some way that seeks to ensure equipment, of an appropriate 'rating' (as defined) be made affordable for persons / businesses, who have special needs; perhaps this may interact with insurances, or other broader considerations linked to social benefits.

Safety Protocols

NOTE: WIP - this needs to be updated from the pre-existing work done, which is focused on a particular type of implementation, rather than the sorts of methods / means / solutions that may be universally applied. It is thought that there will be a market-place of different solutions that have different sorts of safety protocols, providing different sorts of implications, outcomes, etc.

https://docs.google.com/document/d/1VBBFQbjpXeUad_cgu-3TS67GtXZixA5M9nRdkMDU0Y4/edit#

Social Attack Vectors

Started by: Timothy Holborn

Made available as a google-doc for the purpose of encouraging participatory improvement on the 1st of March 2023.

NOTE: Various AI related attack vectors have not yet been documented. One such consideration is what if someone gets confidential information and then provides it to a generative AI system; for the purpose of making the information part of the model, and therefore available to all?

This document has been generated from the content that was originally produced and published online via github into a documentation site: https://devdocs.webizen.org/SocialFactors/SocialAttackVectors/

The intended purpose of this document is to support the means through which safety protocols may be defined for use in human centric AI systems, namely the Human Centric AIsystems; although others are encouraged to produce fit for purpose solutions also. The current information about safety protocols is available via: https://devdocs.webizen.org/SocialFactors/WebScience/SafetyProtocols/ and in-turn also by the corresponding github location. The derivative solutions that are thought to address these and other social attack vectors, are sought to be defined as ‘safety protocols’ which incorporate technical, legal, social and other ecosystem components as to bring-to-effect, the means to significantly reduce harms; and improve accountability and/or presentation of complex issues and related facts, to courts of law.

Introduction

The purpose of the folder on Social Attack Vectors, is to provide definition and illustration of various sorts of behaviours that are interactively undertaken in a manner that can be 'sensed' or influenced by HumanCentricAI technology; and that therefore, are amongst the issues that need to be responded to on a BestEfforts basis, to form a FitForPurpose solution that is better able to address these sorts of issues than may otherwise be the case.

The considerations include CyberAttackVectors as a consequence of their being the product of the efforts or 'semantics' of human beings; as such, the software agents that may be involved in a Cyber Attack Vector are not considered to exist to serve itself.

Each of these sorts of problems need to be considered and solutions that are not dependent upon whether or not public sector workers act appropriately (ie: support criminal prosecutions or probity / hygiene within public sector institutions). Persons should not be required to continue to be in a relationship of dependency with an abuser and/or someone who is shown to be engaging in hostile acts for gainful purposes. Furthermore, circumstances relating to support for GuardianshipRelations and related GuardianshipSemantics deliberations; requires means to support a carer in the event that the person whom they are caring for, becomes involved in a problem that may jeopardise both the person requiring care and in-turn also, the carer. This is not to be considered as any form of approval for abuse within any such guardian/dependent relationship; rather, it is to consider that the appropriation of social attack vectors are most-often executed upon persons that the attacker considers to be vulnerable and that the potential consequences for being identified as having engaged in wrongdoing is low to negligible.

NOTE: Personally, i am mindful of circumstances where persons paid by public funds have engaged in wrong-ful behaviour with serious implications that can never be properly addressed; and that, i have this memory of those who engaged in these sorts of activities, spilling fluids - seeking forgiveness and a continued focus upon their wellbeing - whilst organisationally it was entirely evident that they were set-up to perform Strategic Harms in a manner that was designed to ensure there was no evidence. Protecting Children and other vulnerable people - lawfully, requires means for persons, irrespective of how negatively impacted they are; they may be seriously injured mentally and physically, even thereafter also - made homeless - as the desire of organised behaviours (ie: Public Sector Wrong Doings) seeks to invalidate their lives; yet, these systems - are expressly designed to ensure any such person, can walk into a court of law and through the use of their HumanCentricAI systems - tell the truth and seek help. The consideration is not about the person who gainfully harmed others seeking to make payment via TheSecret in their pity puddle of their own making; rather, it is to ensure that the TheValuesProject delivers a means, that furnishes the opportunity for a judge to make considerations about what it is they observe in relation to evidence provided about a matter (comprehensively); and thereby, depend upon their character and proper use of their most important role in our systems of society, governance and consequentially thereafter also - Peace. This in-turn acts to discourage persons who may otherwise seek to take matters into their own hands, as is a consequence of various forms of war-like behaviour whether declared, well known - or otherwise; which in-turn also, seeks to better support a means to distinguish the circumstances of persons, as is built via the derivative output of TheValuesProject. The WebizenAlliance and instrumentally therein also; TheWebizenCharter is intended to be very clear both by statement and consequential technical apparatus, about rendering support for human right and other related ValuesCredentials. Whilst not all disputes are sought to become the topic of a case that necessarily requires consideration via a court of law; those who gainfully exist via an ideology that is built upon skills to intentionally and unlawfully harm other people for gainful purposes - should find the Human Centric AI ecosystem hostile.

Persons who find themselves in a situation that involves a dispute, should be encouraged to work it out between themselves, yet this is not always feasible and in some cases, it's simply inappropriate. In other systems - a 'command and control' method has been employed, which hsa not demonstrated a capacity to support the human rights of persons very well or in many cases, at all. Conversely, others have sought to produce systems that are entirely confidential and secret. In both cases, there are issues that relate to social attack vectors not being appropriately triageable.

In consideration; the 'balanced' approach seeks to support 'good faith' relations, not as a disability or vulnerability but rather - as a strength. Each individual user, is responsible for defining their own values frameworks, which are in-turn provided support via the Human Centric AI ecosystems and related ValuesCredentials related systems; which are in-turn supported via the SafetyProtocols that support the annunciation of linked semantics.

Summary

Topics include; but are not limited to, Dishonesty, Usury, Exploitation, Abuse, Malfeasance, Social Harms, Deceptive & Misleading Behaviours, Wrongs, Financial Crimes, Corporate Crimes, Attacks Online, Fraud, Social Engineering, etc.

As the ecosystem is intended to be 'human centric' the implications of attack vectors that involve the use of technology (ie: cyber) has been incorporated.....

IMHO: At the end of the day, harm caused to BiosphereOntologies entities is fundamentally caused by other BiosphereOntologies entities, regardless of the SocioSphereOntologies related implications.

There are various forms of Social Attack Vectors, Actions and Activities; that have existed for a very long time, and others that have become a problem in recent decades due to the implications of the use of technology, as does in-turn relate to designs.

So far, i have been able to produce some materials that cover the following sub-topics,

- AttacksOnline
- CriminalActivity
- PublicSectorWrongDoings
- CommercialExploitation
- Dehumanisation
- Dishonesty
- FakeNews
- TemporalAttacks

There is an enormous amount of work to be done in relation to this area, and it will take some time. I also find it to be emotionally exhausting (as noted below); in the meantime, here are some of my thoughts on considerations related to this area of work that is importantly done, to an appropriate level, as to thereafter ensure solutions are illustratively equipped to demonstrate how the ecosystems are intended to work to put a stop to it and/or provide vastly improved means for accessibility to lawful remedy for disaffected persons.

Introduction: Purpose

TheValuesProject seeks to employ various methods, including WebScience and other SocialFactors related considerations to structure methodologies to enable means for people to be better equipped to both benefit from the support of SafetyProtocols and related considerations; a difficult, yet important documentation requirement is to make note of various types of 'social attack vectors', whether they're intended to be addressed via TrustFactory related methodologies or more broadly otherwise (ie; web civics, etc.) it's still important that they're able to be considered somehow.

*Personally, i struggle doing these sorts of tasks and find it very difficult to have a level of comfort about the idea that i've illustrated the problems well enough, or that it is a safe thing to undertake to do; there is both great sadness and an enormous amount of life invested into seeking to be positively responsive towards addressing problems relating to the human rights of others; and in most cases, it can't really be fully discussed publicly. Yet what can be done, is that the underlying principles can be illustrated as a means to support design considerations that denote a level of responsibility that has been so clearly absent from the work done by others. It is all well and good to solely care about 'yourself' selfishly, and not address the means to address problems - but this is neither appropriate nor responsible, nor consistent with the actual fundamental relationship between leadership and the responsibilities that are inextricably linked to the appropriate use of that term as to strive towards living in a manner that is consistent with, what may be considered a fundamental belief in the existence of universal moral values; as is something that has been referred to for consideration by Professor Noam Chomsky... *

https://www.youtube.com/watch?v=iJ2vr2YnSGA

*As I have noted elsewhere, on the 3rd of April 2018 in response to correspondence with Professor Chomsky, as I worked to pursue the development of the ontology related works required to support FreedomOfThought and related requirements. The perceived problem was that whilst many of the W3C CG related folk (including those more broadly whom are involved in such things as WebScience); there was a perceived problem about the lack of social comprehensions in relation to ontological designs; as can in-turn have the effect of perverting the ability for societies to support 'common sense' and persons to have a meaningful relationship with reality. *

Professor Chomsky noted simply;

"The fact that there are pressures and costs does not absolve people of their moral responsibility. The primary custodian of one's actions is oneself."

Yet, as has been demonstrated more significantly in recent years; there are complex underlying factors, that i have sought to address which has the effect of feeding into the HumanCentricDigitalIdentity designs, alongside the broader ecosystems required to support it; as, the fundamental problem becomes, that where people become disassociated as a consequence of the intended behaviours of others, then the problem becomes linked with the importance of the concept to ensure we're working on EndingDigitalSlavery.

*UnderstandingOntologies is of critical importance to gain a better comprehension about the implications and in-turn how they have a foundational basis in built upon science; that can and is in-turn exploited by bad actors (often highly sophisticated ones); as is one of the many forms of Social Attack Vectors that are becoming a greater problem due to AI infrastructure, that is not operating appropriate SafetyProtocols - or at least, that's my opinion. Whilst others may be satisfied and/or happy with the way their ICT systems work for them; the designs brought about via the WebizenTechStack and related applied methods to address SocialFactors via WebScience and otherwise; in-turn leads to complex factors that fundamentally relate to human consciousness. An example of the implications has sought to be illustrated by Henry Strapp in the simplest way I've ever seen done, per below. *

https://www.youtube.com/watch?v=ZYPjXz1MVv0

These sorts of considerations in-turn feed into the ecosystems design paradigms that are embedded into the body of works and the method of assembly relating to the ecosystems tooling, etc.

When considering the intended purpose of constituencies such as TheWebizenCharter, the CommunityOfPractice and other WebizenAlliance CommercialModels that as stated - seek to support the growth of the far broader PeaceInfrastructureProject , Old concepts, whether they be embedded in the systems of faith that people have in all parts of the world; or via old codes of conduct as noted earlier; and indeed also, old terms such as The term Worshipful;

*(a) Honourable, virtuous, of noble character, estimable; highly respectable, decent; of a knight: excelling in knightly virtues, courageous, courteous, of great prowess; maken ~, to honour (sb.); (b) deserving of honour or respect, praiseworthy; also, ?deserving of special treatment, singular [quot. a1500(c1477)]; (c) of an act, a ceremony: demonstrative of due honour or respect; (d)

renowned, eminent, famed; (e) bringing honour or distinction; (f) as noun: one who is honourable, a respectable person. Source: Middle English Compendium

Which does in-turn relate to the term The Honourable as is more commonly used today. The underlying point being that unless there are lawful means to address wrongs that are committed upon people with the express intent of causing that person injury; or indeed also, behaviours that unwittingly or mistakenly caused a person injury; unless there are lawful means to seek remedy, then there is no available means to support Peace.

*As such, I find myself now having to go through the difficult process of describing the nature of some of the horrible things people seemingly seek to gainfully do; involving harms to others. Many of these sorts of issues have existed for a very long time, whilst others have only become a problem or a worse problem due to newer issues.

It is thought that the reason why many of these issues haven't been better addressed is in-part due to the sophisticated nature of what needs to occur to bring about a more comprehensive 'ecosystem solution' to address bad behaviour / bad actors. There are various 'classes' of bad actors which are not the same as one-another. Often they're interactive and often it is unclear which 'category' or 'agent' is best associated with which category.

Due to various forms of vulnerability and the lack of functionality provided to support ValuesCredentials - that is, the ability to support a means where people self-declare what their values frameworks are; and both, what should be expected of them and in-turn also, the relationship.

So, this document and the related group of additional documents on related topics; seeks to illustrate various types of 'attack vectors' and in-turn support the means to consider how it is this environment appropriates a mechanism to provide better 'moral security' and/or alerts and accountability measures that are intended to act in-turn to better support healthy (safe) Relationships(Social), etc.

Description of different types of attacks

Whilst work to more appropriately illustrate the somewhat exhaustive nature of how various types of attack vectors are all too often gainfully employed by bad people and those who've been misled by bad people; none of it is simple, and people who have developed to become professionals in the field employ extremely well-developed and complex methodologies to achieve their objectives - which are generally for personally gainful purposes, at the material expense of others, that may well have consequences relating to serious injury, impairment, disability and/or death of their targets. These sorts of attacks are not simple, and can often evolve in a manner that leads to many different actors getting involved in a broader 'agenda' that serves the interest (at least initially) of the would-be beneficiary.

The consequences are often defined by law to constitute an embodiment of actions and/or behaviours that may be thereby considered an alleged crime; and whilst the proper venue to sort these sorts of things out is a court of law, the apparatus to ensure that avenue for lawful remedy be available, is often actively discouraged by an array of parties; not simply those well known to be involved in crime and/or organised crime.

ChatGPT Contributions

Given one of the prominently employed social attack vectors is to seek to debase the merit of a person's words and/or ability to be heard or be socially supported to be listened to; the use of ChatGPT has been used fairly extensively; including contributions for this topic also

Below is some content that has been generated by ChatGPT.

There are a number of social attack vectors or behaviours that can negatively impact knowledge workers who are working online. Some examples include:

1. Character assassination: Attacking someone's character online, often through spreading false or malicious information about them, can damage their reputation and credibility, and can make it more difficult for them to work effectively.
2. Gaslighting: Manipulating someone into doubting their own perceptions or memories, often through the use of manipulation and deception, can undermine their confidence and make it more difficult for them to speak up or advocate for themselves.
3. Bullying: Using aggressive or abusive behaviour to intimidate or dominate others can create a toxic work environment and make it more difficult for people to do their jobs effectively.
4. Exclusion: Excluding someone from important conversations or decisions, or versioning them out of documentation that they were involved in creating, can undermine their contributions and make it more difficult for them to work effectively.
5. Harassment: Harassment, including sexual harassment, can create a hostile work environment and make it more difficult for people to do their jobs effectively.
6. Discrimination: Discrimination on the basis of race, religion, gender, nationality, or any other protected characteristic can create an unfair and hostile work environment, and can make it more difficult for people to succeed in their careers.

It is important to recognise that these social attack vectors can have serious negative impacts on knowledge workers, and can make it more difficult for them to do their jobs effectively. They can also create a toxic work environment that is harmful to the well-being of workers.

To protect against these types of social attacks, it is important to have clear policies in place to address harassment, discrimination, and other forms of abuse, and to have processes in place for addressing and resolving conflicts. It is also important to create a culture of respect and inclusion, and to encourage open and honest communication. By taking these steps, it is possible to create a more positive and supportive work environment for knowledge workers.

If a target of social attacks is unable to communicate the nature of their circumstances due to law enforcement, legal and/or court processes, or due to threats or fears for their safety, it is important for their employer or organisation to have policies and practices in place to protect them. This may involve providing them with additional support and resources, such as legal assistance or counselling services, to help them navigate the situation.

It may also be necessary to take steps to protect the privacy of the individual and any other persons who may be involved in the situation. This may involve limiting the dissemination of information about the situation and taking steps to ensure that any information that is shared is done so in a way that is consistent with relevant privacy laws and regulations.

In some cases, it may be necessary to involve law enforcement or other authorities to address the situation and protect the safety of the individual and any other persons who may be involved.

Overall, it is important to have a well-defined process in place for addressing and resolving situations where an individual is unable to communicate the nature of their circumstances due to legal or safety considerations, and to provide the necessary support and resources to ensure that the individual is protected.

If law enforcement fails to protect the safety of individuals involved in a situation, it may be necessary to explore other options for addressing the issue. This could involve seeking assistance from other authorities or organisations, such as human rights organisations or NGOs, that may be able to provide additional support and resources.

In some cases, it may be necessary to pursue legal action to hold law enforcement or other authorities accountable for their failure to protect the safety of the individuals involved. This could involve filing a complaint or lawsuit seeking damages or other remedies.

It is also important to consider the safety and well-being of the individuals involved and to take steps to protect them, even if law enforcement is not able to provide the necessary protection. This may involve seeking assistance from friends, family, or other trusted sources, or seeking shelter or other forms of support to ensure the safety of the individuals involved.

Overall, it is important to have a plan in place for addressing situations where law enforcement fails to protect the safety of individuals, and to have the necessary resources and support available to ensure the safety and well-being of those involved.

If a person being attacked has reported the matter to law enforcement but the situation has not yet been resolved and they are subsequently attacked online publicly and/or socially, it is important for those managing online community environments to take steps to protect their human rights. This may involve:

1. Providing support and resources: It is important to provide the person with any necessary support and resources, such as legal assistance or counselling services, to help them navigate the situation.
2. Ensuring their safety: It is important to take steps to ensure the safety of the person being attacked, such as by providing them with access to shelter or other forms of support.
3. Protecting their privacy: It is important to respect the privacy of the person being attacked and to take steps to protect their personal information, especially if they are unable to publish all of the evidence relating to the matter online due to legal or safety considerations.
4. Providing a safe and inclusive environment: It is important to create a safe and inclusive environment for all members of the online community, and to have policies in place to address harassment, discrimination, and other forms of abuse.
5. Encouraging open and honest communication: It is important to encourage open and honest communication and to create a culture of respect and inclusion, where people feel safe and supported in sharing their experiences and concerns.

By taking these steps, it is possible to protect the human rights of individuals who are being attacked online and to create a more positive and supportive online community environment.

It is important to note that in order to effectively protect the human rights of individuals who are being attacked online, it may be necessary to involve law enforcement or other authorities, depending on the nature of the attack and the risks to the individual's safety. It may also be necessary to seek assistance from other organisations or individuals who have expertise in addressing online attacks and can provide additional support and resources.

It is also important to be aware of relevant laws and regulations that may apply in situations where individuals are being attacked online, and to take steps to ensure that the rights of the individuals involved are being protected.

Overall, it is important to take a proactive approach to addressing online attacks and to have the necessary policies and resources in place to protect the human rights of those involved. This may involve providing support and resources to individuals who are being attacked, creating a safe and inclusive online community environment, and working with law enforcement and other authorities to address the situation.

Commercially Motivated Attacks

If the underlying purpose of an attack is commercial or related to financial crimes, and the primary purpose is to obtain an advantage and/or harm the victim in a way that will prevent them from being compensated for their work and cause them injury, it is important for communities involved in work-related activities online to take steps to protect human rights and prevent harm to individuals. This may involve:

1. Having policies in place to address financial crimes and other forms of abuse: It is important to have policies in place that clearly define what types of behaviour are not acceptable and provide guidance on how to report and address incidents of financial crimes or other forms of abuse.
2. Providing support and resources to victims: It is important to provide victims of financial crimes or other forms of abuse with the necessary support and resources, such as legal assistance or counselling services, to help them navigate the situation and recover from any harm they may have suffered.
3. Working with law enforcement and other authorities: It may be necessary to involve law enforcement or other authorities to address financial crimes and other forms of abuse, and to hold perpetrators accountable for their actions.
4. Encouraging open and honest communication: It is important to create a culture of transparency and encourage open and honest communication within the community, as this can help to identify and address issues related to financial crimes or other forms of abuse.

By taking these steps, it is possible to protect the human rights of individuals and prevent harm caused by those seeking to abuse others for financially gainful purposes.

In addition to the steps I listed earlier, there are a few other things that communities involved in work-related activities online can do to protect human rights and prevent harm caused by those seeking to abuse others for financially gainful purposes:

1. Educate members of the community: It is important to educate members of the community about financial crimes and other forms of abuse, and to provide them with information about how to recognize and report these types of incidents.
2. Promote ethical behaviour: It is important to promote ethical behaviour and to encourage community members to act with integrity and respect for the rights of others. This may involve establishing codes of conduct or ethical guidelines for community members to follow.

3. Foster a culture of inclusivity and respect: It is important to create a culture of inclusivity and respect within the community, and to encourage open and respectful dialogue and debate. This can help to create a more positive and supportive environment and reduce the risk of harm to individuals.
4. Monitor and address issues as they arise: It is important to regularly monitor the community for signs of financial crimes or other forms of abuse, and to take prompt action to address any issues that are identified.

By taking these steps, communities can create a more positive and supportive environment for all members, and can help to protect the human rights of individuals who may be at risk of abuse.

If a case or circumstance like this cannot be openly discussed publicly due to privacy, legal, or safety reasons, it can be difficult to provide support and assistance to those involved. In these situations, it may be necessary to take a more discreet approach, and to work with trusted individuals or organisations who can provide the necessary support and resources.

One option may be to seek assistance from organisations or individuals who have expertise in working with victims of financial crimes or other forms of abuse, and who can provide confidential support and resources. This could include legal assistance, counselling services, or other types of support that are tailored to the needs of the individuals involved.

It may also be necessary to work with law enforcement or other authorities to address the situation, while taking steps to protect the privacy and safety of those involved. This could involve sharing information on a confidential basis, or taking other measures to ensure the safety of the individuals involved.

Overall, it is important to be mindful of the privacy, legal, and safety considerations involved in these types of cases, and to work with trusted individuals or organisations to provide the necessary support and resources to those who may be at risk of harm.

If a person is excluded, socially assaulted, and subjected to other broader social, mental, and economic harms as a result of an attack, and the circumstances of the attack cannot be discussed publicly due to privacy and safety issues, it can be difficult to provide support and assistance to the person who has been harmed. In these situations, it may be necessary to take a more discreet approach, and to work with trusted individuals or organisations who can provide the necessary support and resources.

One option may be to seek assistance from organisations or individuals who have expertise in working with victims of social, mental, and economic abuse, and who can provide confidential support and resources. This could include legal assistance, counselling services, or other types of support that are tailored to the needs of the individual.

It may also be necessary to work with law enforcement or other authorities to address the situation, while taking steps to protect the privacy and safety of the person who has been harmed. This could involve sharing information on a confidential basis, or taking other measures to ensure the safety of the individual.

Overall, it is important to be mindful of the privacy and safety considerations involved in these types of cases, and to work with trusted individuals or organisations to provide the necessary support and resources to those who may be at risk of harm.

There are a number of compensation and other measures that could be considered in order to support a code of conduct or community of practice that acts to most benefit people who do the right thing and act in accordance with and support human rights instruments. Some options may include:

1. Financial compensation: In cases where individuals have suffered financial harm as a result of being subjected to social attack vectors, it may be appropriate to provide financial compensation to help them recover from their losses.
2. Legal remedies: In cases where the actions of others have violated the rights of individuals, it may be appropriate to seek legal remedies, such as damages or injunctions, to hold those responsible accountable for their actions and to provide compensation to the individuals who have been harmed.
3. Counselling and support services: It may be necessary to provide counselling and other support services to individuals who have been subjected to social attack vectors in order to help them cope with the emotional and mental trauma they may have experienced.
4. Education and training: Providing education and training on human rights and ethical conduct can help to promote a culture of respect and inclusion, and can encourage individuals to act in accordance with these principles.
5. Policies and procedures: Having clear policies and procedures in place to address social attack vectors and other forms of abuse can help to prevent harm to individuals and create a more positive and supportive community environment.

By considering these and other measures, it is possible to support a code of conduct or community of practice that acts to most benefit those who do the right thing and act in support of human rights, rather than benefiting those who engage in social attack vectors for financial or social gain.

It is also important to have mechanisms in place for addressing and resolving conflicts that may arise within a community of practice, and for holding individuals accountable for their actions. This may involve having processes in place for reporting and investigating incidents of abuse or misconduct, and for taking disciplinary action as appropriate.

It may also be helpful to have resources available for individuals who have been subjected to social attack vectors or other forms of abuse, such as legal assistance or counselling services, to help them navigate the situation and recover from any harm they may have suffered.

Overall, it is important to create a culture of respect and inclusion within a community of practice, and to have policies and procedures in place to address and prevent social attack vectors and other forms of abuse. By taking these steps, it is possible to create a more positive and supportive environment for all members of the community and to ensure that the rights of individuals are respected and protected.

A semantic web ontology is a formal representation of a set of concepts and relationships within a specific domain of knowledge, using a standardised vocabulary and logical rules. In the context of managing social attack vectors, an ontology could be used to represent concepts such as:

- Social attack vector: A specific type of behaviour or tactic that is used to harm or exploit others, either individually or as part of a group.
- Human rights: The fundamental rights and freedoms that are inherent to all human beings, and which are protected under international law.

- Financial crimes: Illegal activities that involve the misuse of financial resources or systems for personal or financial gain.
- Counselling services: Professional services provided by trained individuals to help individuals cope with and resolve emotional, mental, or behavioural problems.
- Legal remedies: Measures that can be taken to address and resolve legal issues, such as damages or injunctions.

By defining these concepts and their relationships within an ontology, it is possible to create a structured and logical representation of the principles for managing social attack vectors, and to use this representation to support decision-making and other processes related to this domain.

Ontology related works

```
@prefix : <http://webizen.org/ns/social/sav.ttl> .

@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .

@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .

@prefix xsd: <http://www.w3.org/2001/XMLSchema#> .



:SocialAttackVector rdf:type rdfs:Class ;

                   rdfs:label "Social attack vector" ;

                   rdfs:comment "A specific type of behaviour or tactic that is used to harm or exploit others, either individually or as part of a group." .



:HumanRights rdf:type rdfs:Class ;

             rdfs:label "Human rights" ;

             rdfs:comment "The fundamental rights and freedoms that are inherent to all human beings, and which are protected under international law." .



:FinancialCrimes rdf:type rdfs:Class ;

                rdfs:label "Financial crimes" ;

                rdfs:comment "Illegal activities that involve the misuse of financial resources or systems for personal or financial gain." .



:CounselingServices rdf:type rdfs:Class ;

                   rdfs:label "Counselling services" ;
                   rdfs:comment "Professional services provided by trained individuals to
help individuals cope with and resolve emotional, mental, or behavioural problems." .


:LegalRemedies rdf:type rdfs:Class ;

              rdfs:label "Legal remedies" ;

              rdfs:comment "Measures that can be taken to address and resolve legal issues,
such as damages or injunctions." .


:ManagingSocialAttackVectors rdf:type rdfs:Class ;

                            rdfs:label "Managing social attack vectors" ;

                            rdfs:comment "The principles and practices for addressing and
preventing social attack vectors and other forms of abuse." .


:FinancialCompensation rdf:type rdfs:Class ;

                     rdfs:label "Financial compensation" ;

                     rdfs:comment "Compensation provided to individuals to help them recover
from financial harm caused by social attack vectors or other forms of abuse." .


:EducationAndTraining rdf:type rdfs:Class ;

                     rdfs:label "Education and training" ;

                     rdfs:comment "Education and training on human rights and ethical
conduct, to promote a culture of respect and inclusion and encourage individuals to act in
accordance with these principles." .


:PoliciesAndProcedures rdf:type rdfs:Class ;

                      rdfs:label "Policies and procedures" ;

                      rdfs:comment "Clear policies and procedures to address and prevent
social attack vectors and other forms of abuse, and to create a more positive and supportive
community environment." .


:ConflictResolution rdf:type rdfs:Class ;

                   rdfs:label "Conflict resolution" ;

                   rdfs:comment "Mechanisms for addressing and resolving conflicts that may
arise within a community of practice." .
```

```
:Accountability rdf:type rdfs:Class ;

                rdfs:label "Accountability" ;

                rdfs:comment "Holding individuals accountable for their actions and taking disciplinary action as appropriate." .


:ManagingSocialAttackVectors .

:FinancialCompensation rdfs:subClassOf :ManagingSocialAttackVectors .

:LegalRemedies rdfs:subClassOf :ManagingSocialAttackVectors .

:CounselingServices rdfs:subClassOf :ManagingSocialAttackVectors .

:EducationAndTraining rdfs:subClassOf :ManagingSocialAttackVectors .

:PoliciesAndProcedures rdfs:subClassOf :ManagingSocialAttackVectors .

:ConflictResolution rdfs:subClassOf :ManagingSocialAttackVectors .

:Accountability rdfs:subClassOf :ManagingSocialAttackVectors .


:SocialAttackVector rdfs:subClassOf :ManagingSocialAttackVectors .

:FinancialCrimes rdfs:subClassOf :ManagingSocialAttackVectors .


:ManagingSocialAttackVectors rdfs:subClassOf :HumanRights .

:SocialAttackVector rdfs:subClassOf :HumanRights .

:FinancialCrimes rdfs:subClassOf :HumanRights .
```

#socialfabric #ValuesFrameworks #SafetyProtocols

Discrimination based attacks.

NOTE: below text is generated by ChatGPT

Discrimination refers to the unequal treatment of individuals or groups based on certain characteristics, such as race, ethnicity, gender, sexual orientation, age, religion, or ability. Discrimination can take many different forms, including:

- Direct discrimination: This occurs when a person is treated less favourably because of a specific characteristic, such as their race or religion.
- Indirect discrimination: This occurs when a seemingly neutral policy or practice has a disproportionate impact on a particular group, such as a requirement for physical dexterity that disproportionately affects people with disabilities.
- Harassment: This occurs when someone is subjected to unwanted and offensive behaviour, such as comments or gestures, that are related to their race, religion, gender, etc.
- Victimisation: This occurs when a person is subjected to adverse treatment because they have made a complaint about discrimination or supported someone else who has made a complaint.

People with disabilities are one group that can experience discrimination. For example, they may face barriers in accessing education, employment, and other areas of life due to physical, attitudinal, and systemic barriers.

Discrimination is contrary to the principles of equality and human dignity, and it is prohibited by many human rights charters, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. These charters establish that everyone is entitled to the same rights and freedoms, regardless of their race, religion, gender, etc.

Unintended Consequences.

It's important to recognize that not all instances of discrimination are intentional or malicious. In many cases, people may not be aware that their behaviour is discriminatory, or they may have unconsciously internalised discriminatory attitudes and biases. This can be especially true when there are differences in cultural backgrounds and perspectives.

For example, in cross-cultural situations, misunderstandings can arise from differences in nonverbal communication, social norms, and cultural values. For instance, a gesture or phrase that is considered friendly in one culture may be perceived as disrespectful in another. In such cases, it is important to approach these differences with openness, respect, and a willingness to learn from one another.

To address these situations, it's important to provide education and awareness-raising about discrimination, cultural diversity, and the importance of treating everyone with respect. This can include:

- Providing training and resources on cultural sensitivity, cultural competence, and the harmful effects of discrimination.
- Encouraging open and respectful dialogue and communication, and providing opportunities for people to learn about and understand different cultural perspectives.
- Promoting a culture of inclusiveness, where everyone feels valued and respected, regardless of their background or cultural differences.
- Encouraging the reporting of incidents of discriminatory behaviour, and providing support and resources for individuals who have experienced discrimination.

By taking these steps, you can help to create an online community where everyone is treated with dignity and respect, regardless of their cultural background. This can help to promote greater understanding, cooperation, and a more peaceful and inclusive online community.

Dishonesty

The broader topic of Dishonesty and/or falsehoods from a perspective of social-attack vectors relates to making communications that are intended to pervert the observers sense of a situation and/or reality; and/or to act in some way that is intended for gainful purposes at the (wrongful) expense of others; and/or, issues relating to these sorts of problems, where there is therefore a desire to be able to enable means to better distinguish the various attributes related to these sorts of problems.

Dishonesty plays a vital role in the performance of other wrongs and/or behaviours that result in harms upon other persons.

Of greater consequence also; is the need to distinguish between persons who honestly held a particular yet false belief about a topic, subject, person - whether it be due to their having been misled, ignorant or in relation to a serious mental illness; vs. those who are intentionally engaging in acts of dishonesty wilfully, for gainful purposes or some other underlying reason that intentionally disregards the consequences those behaviours may injuriously have upon others; and/or consequentially invoke others, to cause harm to the target of a dishonest statement.

A problem linked with these sorts of social attack vectors, is that it may be improper (ie: unlawful) to provide full disclosure about the circumstances of a situation that others are dishonestly making false statements about. These issues do in-turn result in a series of consequences whereby it is difficult to form an appropriate moral and lawful approach to seeking to resolve a problem involving dishonesty, particularly where CriminalActivity may be involved.

Cyber Attack Vectors

Whilst un-developed as yet; a consideration has been made that it may be appropriate to create a category that is separate from the SocialAttackVectors to address risks that more specifically relate to Cyber, although the two areas are in-turn linked. As such, I've relocated the documents about it to be part of the SocialAttackVectors notes.

In the meantime; A collection of resources relating to Cyber is available via these links to the Cyber Folder and Cyber Ops folders of the 'peace project' library.

Attacks Online

ChatAI:

There are many ways that people can engage in attacks to harm others online, often using false or pseudonymous names and identifiers to conceal their identity.

Some common tactics include:

- Harassment: This can include sending threatening or abusive messages, posting hateful or harassing comments, or engaging in online stalking.
- Identity theft: This involves using someone else's personal information, such as their name, address, or social security number, to commit crimes or to impersonate them online.
- Revenge porn: This involves sharing sexually explicit images or videos of someone without their consent, often with the intent to shame or humiliate them.
- Doxing: This involves publicly sharing someone's personal information, such as their address, phone number, or employer, often with the intent to harass or intimidate them.
- Defamation: This involves making false or damaging statements about someone, with the intent to harm their reputation or credibility.
- Cyberbullying: This involves using electronic communications technologies, such as social media or messaging apps, to bully, harass, or intimidate others.

These types of attacks can have serious consequences for the victims, including emotional distress, damage to reputation, and financial losses. It is important for individuals and organisations to be aware of the risks and to take steps to protect against these types of attacks, such as by being cautious about sharing personal information online and by reporting any instances of online harassment or abuse.

In addition to the tactics mentioned above, there are other ways that attackers may use false or pseudonymous names and identifiers to harm others online. Some examples include:

- Spamming: This involves sending unsolicited or unwanted emails or messages, often with the intent to promote a product or service or to spread malware.
- Phishing: This involves using fake emails or websites to trick people into revealing sensitive information, such as login credentials or financial information.
- Impersonation: This involves pretending to be someone else in order to gain access to sensitive information or systems. This can be done through phone calls, emails, or in person.
- Malware: This refers to software that is designed to harm or exploit computer systems, often by accessing or stealing sensitive information or by disrupting the normal functioning of the system.
- Scams: This involves using deception or misrepresentation to defraud people of money or personal information.

Overall, there are many ways that attackers can use false or pseudonymous names and identifiers, as well as private and personal information, to harm others online. It is important for individuals and organisations to be aware of these risks and to take steps to protect against these types of attacks, such as by being cautious about sharing personal information online and by using strong passwords and security measures.

Cyber Crime

OpenAI:

Social Engineering Attacks

Social engineering attacks are a type of cybercrime that involve the use of psychological manipulation or influence techniques to trick people into divulging sensitive information or performing actions that they would not normally do. These attacks rely on exploiting the natural human tendency to trust and to want to help others, and they often target individuals who have access to sensitive information or systems.

There are several types of social engineering attacks, including:

- Phishing: This involves the use of fake emails or websites to trick people into revealing sensitive information, such as login credentials or financial information.
- Baiting: This involves offering something of value, such as access to exclusive content or a free gift, in order to entice people to reveal sensitive information or perform certain actions.
- Scareware: This involves using fear or urgency to persuade people to take certain actions, such as installing software or clicking on a link.
- Pretexting: This involves using a fake identity or pretext to gain access to sensitive information or systems.
- Physical social engineering: This involves using face-to-face or phone interactions to trick people into revealing sensitive information or performing certain actions.

Social engineering attacks can be difficult to detect, as they often rely on psychological manipulation rather than technical vulnerabilities. It is important for individuals to be aware of the risks of social engineering attacks and to take steps to protect themselves from them, such as by being cautious about providing personal information or by verifying the identity of individuals before providing sensitive information.

Some other common social engineering attacks include:

- Impersonation: This involves pretending to be someone else in order to gain access to sensitive information or systems. This can be done through phone calls, emails, or in person.
- Quid pro quo: This involves offering something of value in exchange for sensitive information or access to systems.
- Influence: This involves using persuasion techniques, such as flattery or authority, to convince people to reveal sensitive information or perform certain actions.
- Diversion: This involves distracting people in order to obtain sensitive information or access to systems.

It is important for individuals and organisations to be aware of these types of social engineering attacks and to take steps to protect themselves from them. This can include implementing security measures, such as two-factor authentication and strong passwords, and training employees to recognize and respond to social engineering attempts.

Overall, social engineering attacks are a serious threat to individuals and organisations, as they can lead to the loss of sensitive information and damage to reputation and financial well-being. It is important to be aware of the risks and to take steps to protect against these types of attacks.

Database Attacks

Database attacks may also include knowledge bases, CRMs, etc.

One such form of attack is where false, defamatory or other wrongful statements are created by a database operator that are in-turn intended to be relied upon by others.

The methods employed may involve activities related to StrategicHarms of various kinds and underlying 'incentive' models. Often the underlying intent is to cover-up wrongdoing.. These attacks may in-turn be subject to secrecy agreements, as such the victim of these forms of attacks may not be aware of the information at all; nor have any reasonable means to seek to resolve it.

Other forms of Database Attacks include Hacking / hackers; who may download a targeted database for criminal purposes (ie: extortion, etc) or commercial purpose (ie: using the database information for creating a contact database, etc.)

Unauthorised DeepFakes

The broad concept of DeepFakes refers to the use of technology to create false representations of a person's actions or statements; or to mislead persons via the use of computer generated content that is in-turn disseminated in a manner that is intended to be engendered with FalseAttribution.

The provenance of these sorts of issues pre-date the more expansive implications of behaviours that have historically sought to evoke a response based upon false attribution of a statement or direction; that may in-turn be linked to issues such as those noted by TheSecret alongside others. Yet, through the emergence of advanced technology the ability to modify, alter and/or generate content computationally brings about the means to create synthetic content that may be used positively or negatively.

A positive use-case example is that a content artefact of a person making a speech could be translated to a different language and that the footage of the person making the speech is also modified to support 'lip sync'.

Yet, there are many negative examples that pose great jeopardy, serious implications and require a great deal of WebScience related considerations, in-order to form useful recommendations about how solutions may be best employed.

Technically,

The Human Centric AI ecosystem is intended to provide a capacity for persons to associate themselves with VerifiableCredentials that are able to be used to validate content, and in-turn provide support for 'approved deep-fakes'; whilst also, providing tools that can mitigate some (/ many) risks associated with circumstances where there may otherwise be a lack of capacity to do anything useful and/or that any tools made available to address these sorts of problems, are coupled to other unwanted qualities; that act to compromise the good purposes associated with seeking to address these sorts of issues.

It might be noted; that i am unsure how non-Human Centric AI ecosystems are able to address these sorts of issues as they do not support HumanCentricAI and are consequently impacted by the design implications associated to an ideology that does not support human agency, or in-turn ValuesCredentials and broader ecosystems that are thereby able to be built upon that foundational infrastructure.

Digital Slavery

The concept of Digital Slavery or Web Slavery, is not easily defined - principally as a consequence of the widespread nature of the problem and its many implications. In-order to gain a better understanding of what the intended meaning of forming SafetyProtocols for EndingDigitalSlavery means; the best way i can illustrate the problem now, is to make a note of a few of the very many papers / articles, that have been produced about related topics.

The consideration observers are sought to consider is to ask yourself, if we have such significant AI / Technological capabilities that are equipped to 'know everything', when it suits whoever 'owns' or moreover operates the systems that are collecting and curating the use of this knowledge - then how is it, that these sorts of problems are so endemically problematic?

A short version of a much longer presentation by Eben Moglen (in 2012) who is an American legal scholar who is professor of law and legal history at Columbia University, and is the founder, Director-Counsel and Chairman of Software Freedom Law Center. is below,

https://www.youtube.com/watch?v=9zXqHIJJVxk

Now Therefore;

Digital slavery, time for abolition?

Slavery is a powerful and emotive term describing an abhorrent infringement of fundamental human rights and should not be applied casually. I relate the practice of slavery to two different concepts of “alienation from self”: first, as being “owned” as property by a third party; and, second, as being “owned” in a more informal, contemporary sense, through the removal of an individual’s ability to govern her own life. This dual meaning of alienation from self leads me to consider self-ownership in a legal sense as well as, less formally, as having the agency to determine one’s own life. From both perspectives I claim that the increasing trafficking of personal data to supply algorithm-based analytics and AI is enabling a new form of digital enslavement that has the potential to curtail liberty and cause harm. I suggest that the conceptualization of problematic digital practices as a new form of slavery is a much needed addition to the mainstream critique of the collection, aggregation and trafficking of personal data, which has focused mostly on individual privacy.

This focus, in turn, has obscured and diminished the seriousness of concerns about collective and individual autonomy.

#SlaveTech A snapshot of slavery in a digital age

Thousands of years ago Aristotle wrote that ‘the ox is the poor man’s slave’. But how can an ox be a slave? And how is a slave like an ox? The crucial link is that in this context, both the ox and the human are being used as tools. In fact, Aristotle said exactly that in his book Politics: “some tools are lifeless and others living”, explaining that “for a helmsman the rud- der is a lifeless tool and the enslaved watchman a live tool.” It is not too difficult to think of animals and people as ‘tools’, and while it is less likely we would say an animal or a man is ‘technology’, they are and can be that too. In modern English slang, calling someone a “tool” is a put- down, an insult. And most of us would shy away from so di- minishing a person’s humanity, thereby reducing their personhood, by thinking or saying that another human being is only a tool. Recognition of our common humanity leads us to hate the idea of treating people as things. But that may be why we fail to see how closely linked technology (tools) and slavery can be, and so fail to see how the ox and the slave are similar, and how their differences make the slave the much more profitable and useful of the two.

Modern Indentured Servitude in the Gig Economy: A Case Study on the Deregulation of the Taxi Industry in the United States

Unsustainable business model: The broken promises of Gig economy companies While corporations like Uber pursue intensified vehicular autonomy, that which has lured so many workers to the Gig economy in the United States has been hoped in the American dream through the promise of ongoing employment . In part, jobs driving Uber taxis have been made possible by a seemingly viable business model that became unsustainable all too quickly. Drivers were told they could work for a ride-hailing company like Uber, and they could choose to work whenever they wanted. But what drivers were not told upon signing up, or on leasing or buying a new vehicle to drive for Uber, is that their per mile and per minute rate would be slashed without warning, not once but consecutively. Drivers were not told that they would be left to fend for themselves if things didn't go according to plan and the business model became unviable.

Combating Human Trafficking With Threat Intelligence — Prevention

Eradication of human trafficking requires the expertise, resources, and efforts of many individuals and organisations. It is a complex issue requiring a multifaceted approach set in the United Nations’ Palermo Protocol known as the “4P” paradigm — Prevention, Protection, Prosecution, and Partnership. The 4P paradigm serves as the foundational framework used universally to combat human trafficking.

Combating modern slavery experienced by Vietnamese nationals en route to, and within, the UK

In 2016 the Independent Anti-Slavery Commissioner (IASC) commissioned research to examine the dynamics of Vietnamese nationals' exploitation en route to, and within, the United Kingdom (UK). The research took a mixed method approach and included analysis of National Crime Agency (NCA) National Referral Mechanism (NRM) data, NRM files for 75 Vietnamese victims who had received a positive conclusive grounds (PCG) decision, 61 semi-structured interviews with stakeholders in Vietnam and the UK and 11 life history interviews with Vietnamese potential victims of modern slavery who at the time of fieldwork had received a positive reasonable grounds (PRG) decision. This report presents findings from the research and an executive summary is provided here.

Anti-Human Trafficking Manual for Criminal Justice Practitioners

The *Anti-Human Trafficking Manual for Criminal Justice Practitioners* is the result of a global cooperative process in which expert representatives from academia, NGOs, international organisations, law enforcement officers, prosecutors and judges from all over the world contributed their expertise and experiences.

In line with the Trafficking in Persons Protocol supplementing the United Nations Organized Crime Convention, the purpose of the *Anti-Human Trafficking Manual for Criminal Justice Practitioners* is to support criminal justice practitioners in the prevention of human trafficking, the protection of its victims, the prosecution of its culprits and in the international cooperation needed to achieve these goals.

Are Blockchains Decentralised? Unintended Centralities in Distributed Ledgers

Over the past year, Trail of Bits was engaged by the Defense Advanced Research Projects Agency (DARPA) to investigate the extent to which blockchains are truly decentralised. We focused primarily on the two most popular blockchains: Bitcoin and Ethereum. We also investigated proof-of-stake (PoS) blockchains and Byzantine fault tolerant consensus protocols in general. This report provides a high-level summary of results from the academic literature, as well as our novel research on software centrality and the topology of the Bitcoin consensus network. For an excellent academic survey with a deeper technical discussion, we recommend the work of Sai, et al.

HUMAN IDENTITY: THE NUMBER ONE CHALLENGE IN COMPUTER SCIENCE

Human identity is essential and complex. It is essential to sense-making and cooperation and so then to the fundamental processes of human life. It is complex in its operations and so in its descriptions; it means different things to different people in different contexts. In light of the deep digitalization of our world, developments in computer science affect everyone. Many applications of computer science concern people and relationships, our interactions with each other and with digital technology, and with our cyborgian extension, and so I can only consider the diligent digital mediation and augmentation of human identity to be the discipline's foremost challenge. Historic systemizations of identity have brought advantages and disadvantages, great benefits and grave harms, and I have this in mind when observing computer scientists currently developing protocols and technologies to systematise a narrow conceptualization of identity at scales and with a potential intensity never before contemplated let alone pursued. We need to have a deeper think about this.

Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID

The Digital Welfare State and Human Rights Project originally emerged from our support of the mandate of the United Nations Special Rapporteur on extreme poverty and human rights. The initial focus was on the digital transformation of welfare states in the Global North, including in the United States and United Kingdom.1 However, during the preparation of the 2019 Special Rapporteur's report to the UN General Assembly on digital welfare states,2 many practitioners and academic experts drew our attention to a specific model of digital identification systems, frequently with biometric components (digital ID systems), which is being deployed by national governments in the Global South. Recognizing that these systems raise major human rights concerns that go far beyond the realm of Northern welfare states, we have spent the past few years increasingly engaged in national and international debates on digital ID.

Human and Machine Consciousness

Consciousness is extremely important to us. Without consciousness, there is just nothingness, death, night. It is a crime to kill a person who is potentially conscious. Permanently unconscious people are left to die. Religious people face death with hope because they believe that their conscious souls will break free from their physical bodies. We know next to nothing about consciousness and its relationship to the physical world. The science of consciousness is mired in philosophical problems. We can only guess about the consciousness of coma patients, infants and animals. We have no idea about the consciousness of artificial systems.

The Age of Digital Interdependence

Digital technologies are rapidly transforming society, simultaneously allowing for unprecedented advances in the human condition and giving rise to profound new challenges. Growing opportunities created by the application of digital technologies are paralleled by stark abuses and unintended consequences. Digital dividends co-exist with digital divides. And, as technological change has accelerated, the mechanisms for cooperation and governance of this landscape have failed to keep pace. Divergent approaches and ad hoc responses threaten to fragment the interconnectedness that defines the digital age, leading to competing standards and approaches, lessening trust and discouraging cooperation.

Crypto & DeFi Hacks, Fraud & Scams Report

Despite the constant evolution and maturation of blockchain technology and the crypto market, 167 attacks on Decentralised Finance protocols, 123 security attacks, and 74 fraudulent schemes over the last 11 years have so far resulted in the theft of approximately USD $14.58 billion worth of cryptocurrency assets in total at the time of writing this report (July 2022).

The Promise and Perils of International Human Rights Law for AI Governance

The use and deployment of artificial intelligence (AI) presents many challenges for human rights. Consequently, the search for an AI governance framework has led to a relatively recent proliferation of government strategies, corporate ethics codes, engineering design ethics, and international regulatory frameworks that seek to regulate its application. For purposes of this paper, AI—a term that has no consensus definition in technology and policy making circles1—refers to a complex information system that approximates behaviour commonly understood as requiring intelligence, similar to human behaviour, such as pattern recognition, logical reasoning, or language processing.

The Commodification of Knowledge and Information

In this paper we present an analysis of the commodification of knowledge and information in contemporary capitalism. We provide a consistent account of how information as a commodity affects the workings of both capitalism and of Marxist theory. The first part of the paper critically revisits Marx's own writings on the commodification of knowledge and how the immaterial labour hypothesis initially interpreted these writings. Based on the new categories knowledge-commodity and knowledge-rent, we then present our own approach in response to the challenges raised by the immaterial labour hypothesis. Lastly, we analyse the more recent contributions on the commodification of knowledge and information within the Marxist literature. The current debate on the value of knowledge has been divided between two camps: the reproduction cost approach, and the average cost approach. At the end of the paper we present empirical estimates of the magnitudes of knowledge-rents.

Beyond Data Alessandro Mantelero Foreword by Prof. Joe Cannataci Human Rights, Ethical and Social Impact Assessment in AI

It is probably safe to say that at the time of writing1 more than 99% of the world's population do not yet understand what a game-changer AI can be...or is already proving to be. Much news coverage, for example, is still given to efforts which aim to prevent states like Iran or North Korea from developing nuclear weapons and increasingly sophisticated means of delivering them. Yet relatively little news coverage is given to the fact that, in reality, AI has made nuclear weapons obsolete. Why would a state—or indeed a terrorist—wish to deploy or acquire a very expensive and relatively unstable nuclear weapon when it can instead deploy much cheaper AI-controlled devices which do not create a radioactive crater or destroy so many valuable assets in a target zone?

White Paper eDATA Verifiable Credentials for Cross Border Trade

The international supply chain is growing in complexity at the same time as nation states seek to improve their border compliance for imports and facilitate access to export markets for their domestic producers. The global value chain is highly dependent on smooth cross-border supply flows (tangible, intangible, and data). In an uncertain world that is buffeted by rapid technological change, environmental and health crises, and political uncertainties, national policies can have significant impacts on cross border trade challenges.

The "cost of trade"2 roughly doubles the landed price of goods in export markets (compared to domestic wholesale prices) with around one third of that cost related to non-tariff border costs. Nations that can reduce their cost of trade with their trading partners will confer a significant comparative advantage for their exporters and thereby improve the national balance of trade.

- At around $1.7 Trillion USD, the trade finance gap (i.e. trade finance requested but not approved) is heavily weighted against small and medium enterprises (SMEs) and acts as one of the most significant barriers to SME participation in cross-border trade. Nations who can uplift SME participation rate in cross border trade will experience greater growth and improved balance of trade.

- At around 3% of world trade volume, the value of fake / illicit goods trade is at least $600Bn and rising. The consequences include market losses for exporters of genuine goods and potential reputational damage for entire market segments. Nations who can help their exporters prove the authenticity of goods will enjoy a comparative advantage over those that do not.

· With annual carbon emissions at around 25 billion tons5 and with approximately 25 million people in forced labour, and 400 million tons of hazardous waste produced annually, there is a rapidly increasing consumer demand for sustainable products. Nations that can prove the sustainability of their exported goods through verifiable supply chain transparency will enjoy both higher prices for their goods and lower tariffs as importing nations start to penalise un-sustainable imports.

· With border authorities only able to inspect around 1% of around 1 billion sea containers8 and a much smaller proportion of 100 billion parcel shipments per year, the challenge of managing border risk against illicit goods and biosecurity threats has never been greater. Nations that can leverage high integrity data about import consignments can both increase seizures and facilitate legitimate imports.

The challenges described above are quite significant. Equally, the opportunities for nations that can address these challenges more effectively than their competitors are also significant. Digitisation is a key enabler of all strategies to address these challenges. Although many nations have made significant progress in digitising trade processes within their borders such as implementing trade single windows, there remain significant challenges in digitising cross-border processes.

Diverse regulatory models and priorities across nations amplify the challenge. National policy making will reflect a complex mixture of market-oriented, security-oriented, rights-oriented, and domestic development-oriented priorities. These differences lead to problems of compatibility or interoperability among nations, and fragmentation of the digital space at the global level. Any scalable solution to the digitisation of cross border trade must embrace and not conflict with diverse policy making priorities.

This paper describes a highly scalable operating model for digitisation and trust of cross border trade based on verifiable credentials, linked data, and decentralised identifiers. It provides national regulators with implementation guidance that will facilitate the following outcomes.

Artificial Intelligence and the Future of Humans

Experts say the rise of artificial intelligence will make most people better off over the next decade, but many have concerns about how advances in AI will affect what it means to be human, to be productive and to exercise free will

MisRepresentation

This note about MisRepresentation attack vectors notes circumstances where a person may use a 3rd party identifier/ accounts and perform activities on that account in a manner that is intended to mislead other persons to believe it was the account holder undertaking those activities, rather than the attacker.

There are various examples of where this may be employed as part of a broader attack.

Some examples are more closely related to CriminalActivity and wrong-doings seeking to cause injury, however others may simply be circumstances such as instances where children make use of their parents accounts to make purchases or perform other activities online that they're unable to do themselves alone.

Nobody AI

The concept of Nobody AI refers to AI and/or software solutions that are designed in such a way whereby the use of those systems may cause harm to others; but that it is the fault of no human being - by design. The implication being that companies and software agents can be used to knowingly harm others, in a manner that is designed to seek to ensure there are no penalties applied upon any human beings as a consequence of how those systems impact other human beings, as a consequence of the design of how #NobodyAI is intended to be operated - by the human beings that have designed those systems.

"All Care, no responsibility. #NoBodyAI"

Some Illustrative Examples:

Ie: like robodebt (LINK1 LINK2); or say for example, You lost your child because the government made a bunch of mistakes? so, after the irreversible consequences have played out; and an opportunity for the situation to be reviewed occurs (noting - this is a fictional use-case) many years down the track; the OFFICIAL answer becomes,

oh, that was the fault of nobody; Yes, we're all paid / compensated in our jobs working for the government; but, we've made this AI system, that means we're never responsible for anything that happens to anyone. it's our #NobodyAI platform - that will do whatever we tell it to do to you, and if that's bad or if you make enough noise about it; the enquiry, the court, whoever is asking questions will be told clearly - it was no-bodies fault, the decisions were all made by our #NobodyAI platform. if you have a problem with that - take it up with the department of responsibility... Which is probably, run out of the US via another AI platform.

The Human Centric AI ecosystem is the opposite of a NobodyAI design and any such form of related ecosystem.

Tech Debt

ChatGPT used to provide definition

MyQuestion; describe the concept "Tech Debt"

ChatGPT: "Tech debt" is a metaphor used to describe the cost of maintaining and updating technology systems. It refers to the trade-off between short-term gains and long-term costs when making decisions about how to design, develop, and maintain technology systems.

Tech debt is incurred when a team chooses to take shortcuts or make compromises in order to deliver something quickly, but at the cost of making it more difficult or expensive to maintain or modify in the future. For example, using a quick-and-dirty solution to a problem instead of taking the time to design a more elegant, maintainable solution would be considered taking on tech debt.

Tech debt can also be incurred when a team is under pressure to deliver something quickly and doesn't have the time to implement best practices or follow industry standards. This can lead to code that is hard to understand or maintain, making it more difficult to add new features or fix bugs in the future.

The interest on tech debt is the cost of maintaining the software or system. This can include the cost of fixing bugs, adding new features, or making changes to the system. The longer the debt is unpaid, the more the interest compounds and the more expensive it becomes to maintain the system.

In summary, "Tech debt" refers to the cost of maintaining and updating technology systems. It occurs when a team chooses to take shortcuts or make compromises in order to deliver something quickly, but at the cost of making it more difficult or expensive to maintain or modify in the future. It's important to balance the short-term gains and long-term costs when making decisions about how to design, develop, and maintain technology systems.

My Question: What are the Cyber Security Risks and Threats that are brought about as a consequence of Tech Debt?

ChatGPT:

Tech debt can introduce a variety of cyber security risks and threats, some of which include:

1. Vulnerabilities: Tech debt can lead to vulnerabilities in the system, such as poor code quality or a lack of testing. These vulnerabilities can be exploited by attackers to gain unauthorised access to sensitive data or take control of the system.
2. Unpatched software: Tech debt can make it more difficult to keep software up to date with the latest security patches. This can leave systems open to known vulnerabilities that have already been fixed in more recent versions of the software.
3. Outdated software: Tech debt can also make it more difficult to upgrade to newer versions of software, which may have better security features. This can leave systems open to newer threats that have emerged since the software was last updated.
4. Lack of monitoring: Tech debt can make it more difficult to monitor systems for suspicious activity. This can make it harder to detect and respond to cyber attacks in a timely manner.
5. Lack of compliance: Tech debt can make it difficult to comply with regulations and industry standards for data security. This can lead to fines and reputational damage for the organisation.
6. Difficulty in incident response: Tech debt can make it difficult to quickly detect a security incident and respond to it, which can prolong the incident and increase the damage caused by it.
7. Difficulty in performing security testing: Tech debt can also make it difficult to perform security testing on systems and applications, as the complexity and lack of maintainability of the codebase can make it hard to identify vulnerabilities or simulate realistic attack scenarios.

8. Difficulty in understanding the attack surface: Tech debt can make it difficult to understand the attack surface of the system, which can make it harder to identify and prioritise vulnerabilities that need to be addressed.
9. Difficulty in implementing new security controls: Tech debt can make it difficult to implement new security controls, such as encryption or multi-factor authentication, as the complexity and lack of maintainability of the codebase can make it hard to integrate new features.
10. Difficulty in incident response: Tech debt can also make it difficult to perform incident response, as the complexity and lack of maintainability of the codebase can make it hard to identify the cause of an incident, understand the scope of the incident, and implement countermeasures.
11. Difficulty in forensic analysis: Tech debt can make it difficult to perform forensic analysis on systems and applications, as the complexity and lack of maintainability of the codebase can make it hard to understand the state of the system at the time of an incident.

Tech debt can lead to a variety of cyber security risks and threats, such as vulnerabilities, unpatched software, outdated software, lack of monitoring, lack of compliance, and difficulty in incident response. It's important for organisations to manage and mitigate tech debt to minimise these risks and protect their systems and data from cyber attacks.

In summary, Tech debt can introduce a variety of cyber security risks and threats such as vulnerability, unpatched software, outdated software, lack of monitoring, lack of compliance, difficulty in incident response, difficulty in performing security testing, difficulty in understanding the attack surface, difficulty in implementing new security controls, difficulty in forensic analysis and so on. It's important for organisations to manage and mitigate tech debt to minimise these risks and protect their systems and data from cyber attacks.

Permanent Identifiers

Some protocols do not support the ability to remove a record once it has been submitted to that protocol. These sorts of features are of fundamental functional importance for the useful application of some protocols.

However, this function can be used as an attack vector; whereby harmful statements and/or media may be uploaded to a protocol for the purpose of instigating an enduring attack upon a person that cannot be removed.

This might include revenge porn and an array of other examples that may have an enduring effect upon the victim.

The other issue related to these sorts of attack vectors is that the content may be consumed by software agents and incorporated into their knowledge models as facts.

Strategic Harms & Exploitation

I have created a sub-folder about topics and/or methods of Social Attack Vectors, that require one or more persons to make conscious decisions to employ a strategy that is intended to gainfully deliver some sort of outcome at the express cost of others.

The genesis of these sorts of events are generally associated with intended behaviours, that those who engage in these sorts of behaviours are 'gamifying' a circumstance in a manner that is strategically defined to result in an outcome where their potential downside is limited whilst the upside engenders value for those who do it; and particularly therein/thereafter, those who are skilled in these sorts of practices.

The outcome being a situation where harms are engendered upon others in a manner that has the effective inference of knowingly Dehumanisation a target on the basis that if they are found-out - then its a situation of *'what are you going to do about it?'*, therein leveraging broader circumstances where access to justice, lawful remedy is mute or engendered in such a way whereby the costs of seeking remedy outweigh any benefit.

Gamification is the strategic attempt to enhance systems, services, organisations, and activities by creating similar experiences to those experienced when playing games in order to motivate and engage users.[1] This is generally accomplished through the application of game-design elements and game principles (dynamics and mechanics) in non-game contexts.[2][3]

Source: WikiPedia

These sorts of attack vectors require Dishonesty and are closely aligned with Torts, CyberAttackVectors, CommercialExploitation and CriminalActivity. Those who are adapt at these sorts of activities often do so, in relation to a belief system that influences how it is that they engage in the behaviour and whom they engender these sorts of tactical processes upon; whilst others, may not find the idea that any such person could ever be considered to act in such a way, which is most often associated with privilege.

The underlying rationale; is oftentimes fairly unsophisticated, and motivated by economic considerations; therein, persons who have a capacity to employ others as to triage a threat effectively - are unlikely to be victims of these sorts of persons and/or behaviours directly, although the repercussive effects may well lead to major problems.

Academic / Institutional Funnelling

These sorts of attack vectors are described in relation to CommercialExploitation mechanisms; where the objective of the attacker is to engender benefit indirectly.

This may include Manipulation, Dehumanisation, PublicSectorWrongDoings, works to Compromise and engender Impairment whilst delegating AuthorisedThinkers who may in-turn be young, yet enthusiastic yet overwhelmingly otherwise - somewhat innocent (and often also - not treated well themselves!).

By funnelling works via FalseAttribution related tactics into large institutions, the institutions provide a barrier and/or defence framework, that protects any underlying person who is wilfully engaged in StrategicHarms and perhaps also CriminalActivity.

The use of Academic or institutions to funnel activities that are built upon wrongs; through the use of students as a form of proxy that is intended to support an agenda for gainful purpose; whilst leading to the misuse of students or other naive persons as pawns; which, when related to CriminalActivity and an underlying intent to mitigate possibility of consequences and/or prosecution, etc. is a particularly complex problem.

Authorised Thinkers

The "Authorised Thinker" paradigm often relates to sophisticated actors who engage in whatever activity required to assign someone else's work to be progressed by the 'Authorised Thinkers' who are then delegated to be publically considered the creators and/or inventors of whatever body of work that is sought to be progressed by underlying 'shadow directors'. These attack vectors often relate also to PublicSectorWrongDoings and CommercialExploitation.

Brain Rape

Intellectual property robbery thinly disguised as acquisition talk. Usually committed by a big company on a startup. Yelp got brainraped by Google back in the day. source: https://svdictionary.com/words/brain-rape

The illustration of the concept comes from the show Silicon Valley. I can't find a better copy of the video atm - if / when I do, I'll update the link...

https://www.youtube.com/embed/ernszq3Xjq4

Commercial Exploitation

The concept of commercial exploitation seeks to distinguish between 'competition' vs. exploitation, Dishonesty, Dehumanisation, TemporalAttacks and various other activities that intentionally disregard the fundamental rights and obligations (ie: fair-dealings, etc) of both directors and the the consequences upon the target of these sorts of behaviours, whether it be done by public or private sector individuals.

The secondary issue relating to these sorts of behaviours is that the consequential 'cover-ups' can invoke a series of behaviours and related outcomes that are actually far worse than the consequence of wrong-doing in the first instance, by whomever it was that did it.

It is common for this sort of thing to occur in relation to TemporalAttacks, that is that a person does a bunch of work which effectively articulates something that is able to be considered an opportunity by the recipient / observer; and then, they engage in acts of Dishonesty and sometimes also either or both; Dehumanisation, AttacksOnline and CriminalActivity in-order to secure the commercial benefit for progressing the works produced by the target of these attacks; by way of appropriating the means to gain contractual value (often also involving non-disclosure / confidentiality / secrecy agreements); at the expense of the target. In some cases this may also result in the target being intentionally and secretively prevented from gainfully benefiting from the use of their own work as was created at the time of the exploitation event, and as may also be engendered to continue in perpetuity.

Which is in-effect, a form of slavery or indentured servitude or other form of CriminalActivity; that may then have been endorsed by others, who collectively seek to extinguish any liability associated with their behaviours, which is likely to cause serious injury to the target and may even lead to death; or in other circumstances, it may invoke a situation where the target resorts to CriminalActivity due to there being no available lawful remedy, by design.

Commercial exploitation is different to competition; the difference is that there are behaviours that are knowingly wrong and thereby breach various laws and international instruments used in connection to law; even if, it is considered to be a common practice.

The main determining factor that denotes a relationship between any other form of SocialAttackVectors and the notions related to Commercial Exploitation; is where the activities specifically relate to a Gainful outcome being engendered by those engaged in the attacks; either directly or indirectly, irrespective of how complex the underlying factors may be.

There are many very serious CriminalActivity issues that relate to these sorts of wrongs.

(These sorts of issues absolutely relate the fundamental purpose of Human Centric AIto provide an alternative ecosystem for persons who do not want to be part of these mob like activities)

Compromising

Compromising an agent is a form of Manipulation and relates to TemporalAttacks.

In relation to CriminalActivity and CommercialExploitation attacks, the use of vulnerable people may be employed for the express purpose of seeking to exert a Manipulation attack that has an intended series of implications that may be used to threaten and/or invalidate the target.

Dehumanisation

ChatGPT Description

Q: Define Dehumanisation?

Dehumanisation is the act of treating people as if they are less than human, or of depriving them of human qualities or characteristics. It can involve denying people their basic rights and freedoms, or treating them as objects or animals rather than as individuals with dignity and worth. Dehumanisation can have serious consequences, as it can lead to discrimination, violence, and other forms of abuse. It can also have psychological and emotional impacts on those who are dehumanised, as it can cause them to feel degraded, marginalised, and disconnected from society. Dehumanisation is often associated with prejudice, discrimination, and other forms of social injustice, and it is considered to be a serious violation of human rights.

Q: What are some sorts of commercial and/or public sector behaviours that act to dehumanise targeted victims?

There are many different behaviours that can contribute to the dehumanisation of targeted victims, including:

1. Denying people their basic rights and freedoms, such as the right to education, healthcare, or a fair trial.
2. Treating people as objects or commodities, rather than as individuals with their own unique needs and desires.
3. Using language or imagery that is degrading or offensive, or that portrays people in a negative or stereotypical way.
4. Engaging in violence or other forms of physical abuse against people.
5. Discriminating against people on the basis of their race, ethnicity, gender, sexual orientation, or other characteristics.
6. Using propaganda or other forms of media to spread misinformation or to manipulate public opinion about certain groups of people.
7. Enacting laws or policies that disproportionately harm or disadvantage certain groups of people.

These behaviours can take place in both commercial and public sector contexts, and they can have serious consequences for the targeted victims, including physical harm, emotional distress, and economic hardship.

Fake News

The concept of 'Fake News' fundamentally relates to a content artefact that seeks to make representations that are sought to be consumed as #Non-Fiction assets, when in-fact it is either a complete work of #Fiction or incorporates #fictionalReferences or #Opinions or other content that is not in-fact - #Fact or as is otherwise defined - #NonFiction.

This in-turn relates to the functions and processes related to categorisation of content using genres and other categories / category theory related techniques.

False information does not necessarily infer that it must have been done with malice. There are various #modal considerations related to the management of artefacts that have complex systemic factors associated with them. Nonetheless, this area of social attack vectors can have seriously harmful consequences; and the most dangerous future types of these sorts of attacks may well be carried out by #AiAgents in a personalised manner, which is intended to invalidate FreedomOfThought related principals.

Summary of Considerations

Whilst the term commonly used by media is 'fake news' the underlying issues relate to representations that may be intentionally false and misleading and intended to elicit or engender a particular response or act to pervert the ability of persons to gain a comprehension of a situation that is consistent with the actual facts of a matter. This also relates to various forms of TemporalAttacks and other SocialAttackVectors more broadly.

The underlying notion of 'fake news' may be due to various underlying circumstances; and the way in which any records are updated are in some ways as important to address, as the underlying issues that may relate to the original statements having been improperly communicated. Fundamentally, the concept relates more broadly to Dishonesty, which is a problem that is far greater than the effect of what occurs via news media content alone.

EliPariser Google Docs contribution by me

Around November 2016 Eli Pariser produced an Open Google Document to seek out collaborative support for solutions to address fake-news. Around that time, I made some contributions. A News Article from wired talks about the situation and google doc (noting, it's important to review the historical versions of the document as its often defaced)

A version of my contributions are provided below (I'm unsure if or how it's been altered); noting that the content was authored to highlight solutions rather than the problem.

Considerations → Principles → The Institution of Socio - Economic Values

by: Timothy Holborn

A Perspective by Eben Moglen from re:publica 2012

The problem of ‘fake news’ may be solved in many ways. One way involves mass censorship of articles that do not come from major sources, but may not result in news that is any more ‘true’. Another way may be to shift the way we use the web, but that may not help us be more connected. Machine-readable documents are changing our world.

It is important that we distil ‘human values’ in assembly with ‘means for commerce’. As we leave the former world of broadcast services where the considerations of propaganda were far better understood; to more modern services that serve not millions, but billions of humans across the planet, the principles we forged as communities seem to need to be re-established. We have the precedents of Humans Rights, but do not know how to apply them in a world where the ‘choice of law’ for the websites we use to communicate, may deem us to be alien. Traditionally these problems were solved via the application of Liberal Arts, however through the advent of the web, the more modern context becomes that of Web Science incorporating the role of ‘philosophical engineering’ (and therein the considerations of liberal arts via computer scientists).

So what are our principles, what are our shared values? And how do we build a ‘web we want’ that makes our world a better place both now, and into the future?

It seems many throughout the world have suffered mental health issues as a result of the recent election result in the USA. A moment in time where seemingly billions of people have simultaneously highlighted a perceived issue where the results of a populous exacting their democratic rights resulted in global issues that pertained to the outcome being a significant surprise.   So perhaps the baseline question becomes; how will our web better provide the means in which to provide us (humans) a more accurate understanding of world-events and circumstances felt by humans, via our ‘world wide web’.

**# Linked-Data, Ontologies and Verifiable Claims

By: @Ubiquitous

Linked-Data is a technology that produces machine and human readable information that is embedded in web pages. Linked-Data powers many of the online experiences we use today, with a vast array of the web made available in these machine-readable formats. The scope of linked-data use, even within the public sphere, is rather enormous.

Right now, most websites are using ‘linked data’ to ensure their news is being presented correctly on Facebook and via search, which is primarily supported via Schema.org .

The first problem is: that these ontologies do not support concepts such as genre. This means in-turn that rather than ‘news’ becoming classified, as it would in any ordinary library or newspaper, the way in which ‘news’ is presented in a machine-readable format is particularly narrow and without (machine readable) context.

This means, in-turn, that the ability for content publishers to self-identify whether their article is an ‘advertorial’, ‘factual’, ‘satire’, ‘entertainment’ or other form of creative work - is not currently available in a machine-readable context.

This is kind of similar to the lack of ‘emotions’ provided by ‘social network silos’ to understand ‘sentiment analysis’ through semantic tooling that offer means to profile environments and offer tooling for organisations. Whilst Facebook offers the means to moderate particular words for its pages, this functionality is not currently available to humans (account holders).

The mixture of a lack of available markup language for classifying posts, alongside the technical capabilities available to ‘persona ficta’ in a manner that is not similarly available to Humans, contributes towards the lack of ‘human centric’ functionality these platforms currently exhibit.

Bad Actors and Fact-Checking

In dealing with the second problem (In association to the use of Linked-Data), the means in which to verify claims is available through the application of ‘credentials’ or Verifiable Claims which in-turn relates to the Open Badges Spec.

These solutions allow an actor to gain verification from 3rd parties to provide their audience greater confidence that the claims represented by their articles. Whether it is the means to “fact check” words, ensure images have not been ‘photoshopped’ or other ‘verification tasks’, one or more reputable sources could use verifiable claims to in-turn support end-users (reader / human) to gain confidence in what has been published. Pragmatically, this can either be done locally or via the web through 3rd parties through the use of Linked-Data. For more information, get involved in W3C, you’ll find almost every significant organisation involved with Web Technology debating how to build standards to define the web we want.

General (re: Linked Data)

If you would like to review the machine-readable markup embedded in the web you enjoy today, one of the means to do so is via the Openlink Data Sniffer An innovative concept for representing information was produced by Ted Nelson via his Xanadu Concept

Advancements in Computing Technology may make it difficult to trust media-sources in an environment that seemingly has difficulty understanding the human-centric foundations to our world; and, where the issues highlighted by many, including Eben Moglen, continue to grow. Regardless of the technical means we have to analyse content, it will always be important that we consider virtues such as kindness; and, it is important that those who represent us, put these sorts of issues on the agenda in which “fake news” has become yet another example (or symptom) of a much broader problem (imho).

A simple (additional) example of how a ‘graph database’ works as illustrated by this DbPedia example. The production of “web 3.0” is remarkably different to former versions due to the volume of pre-existing web-users. Whilst studies have shown that humans are not really that different, the challenge becomes how to fund the development costs of works that are not commercially focused (ie: in the interests of ‘persona ficta’) in the short-term, and to challenge issues such as ‘fake news’ or indeed also even, how to find a ‘Toilets’. As ‘human centric’ needs continue to be unsupported via the web or indeed also, the emerging intelligent assistants working upon the same datasets; the problem technologists have broadly produced becomes that of a world produced for things that ‘sell’, without support for things we value. Whether it be support for how to help vulnerable people, receipts that don’t fade (ie: not thermal, but rather machine-readable), civic services, the means to use data to uphold ‘rule of law’, vote and participate in civics or the array of other examples in which we have the technology, but not the accessible application in which to apply the use of our technology to social/human needs.

Indeed the works we produce and contribute on the web are for the most-part provided not simply freely, but at our own cost.   The things that are ‘human’ are less important and indeed, poorly supported.**

False Attribution

Activities relating to False Attribution; includes but is not limited to, Plagiarism, CommercialExploitation, Dishonesty, FakeNews and various other techniques that have various implicit and explicit implications.

An agent engaged in activities that relate to False Attribution are unable to show the provenance of the work in question extending prior to the works that it is based upon.

These issues are often linked to the problems described by TheSecret

NOTE: This needs to be expanded upon more - WIP TODO LIST...

Impairment

An Impairment attack vector is a form of organised behaviour where the objective is to engender circumstances where the target is no longer able to pursue works that others may not want to happen, may consider to give rise to jeopardy of being 'found out' (ie: CriminalActivity / FinancialCrimes) or may also relate to personal circumstances.

The objective process will seek to ensure that the target is made incapable.

Impairment attacks may include obstructive behaviour and/or strategic works that seek to instigate circumstances where the person becomes flooded with problems, Revoking their ability to earn income / obtaining / removing their customer base / income sources.

These sorts of methods are supported by various TemporalAttacks vector issues, whereby the ability to remedy the consequences of these attacks, is often not viable as a consequence of the amount of time it takes to address the repercussive implications of the attack; whilst those involved in prosecuting the attack, benefit and progress. Where this relates to CommercialExploitation the mechanisms often seek to engage many others as to engender a situation where the cost of addressing the problem becomes prohibitively high which thereby employs Manipulation tactics to support organised endorsement and support for the carriage and maintenance of the attack, which may have various implications upon the victim; including but not limited to, Dehumanisation and other various issues that fundamentally relate to CriminalActivity.

Manipulation

Manipulation as a social attack vector, is executed via many different ways.

Often also, there's entrapment involved.

The broader objective is generally about CommercialExploitation.

You Must Be Famous!!!

This topic, refers to issues that link Privacy, Dignity to other human rights and related broader Values related considerations which is the topic of TheValuesProject.

There should be no unreasonable requirement for persons to become public property and/or 'famous' as a predicate or requirement put upon them to be furnished rights.

These attack vectors are commonly associated with KnowledgeWork related issues. It can be the case where external actors seek to engender controls by either or both, exploiting persons who are not well known publicly; or, defining persons via media and publically otherwise or claiming that they are not suited to that form of approach, which is in-turn employed for various activities related to CommercialExploitation.

Whilst there is a distinction between the importance of ensuring Accountability and Responsibility, this does not necessarily require a person to be made publicly known for the field of endeavour and/or work that is implicitly considered valuable enough; to warrant any such form of attack vector thereafter being employed, by others.

Agency & Choice

The choice to form and define oneself within the public domain invokes a series of implications that can often be a mixed blessing. some remark that the nature of the situation leads to persons being considered by others a form of public property.

In other circumstances, the nature of the endeavour may be of a kind that relates to personal and private matters that may have invoked the underlying motivation of the person to do work that may address any such form of 'issue' (social, economic, etc.) but that the intended outcome wasn't about being publically 'owned' via media; but rather, an effort that sought / set-out to address an underlying problem, that would generally at the stage that this sort of attack vector becomes a problem - is garnishing support.

The choice, whilst best sought to be informed - which is to some-degree outside of the scope of these projects; should be held by the person whom any such decision relates to.

A person's rights and obligations should not be predicated upon whether or not they are 'famous'. Conversely also, those who are famous, should not be required to declare themselves in-order to be treated with respect and dignity; which is sometimes better found in circumstances where they are not required to expose who exactly they are.

Solutions matrix

These sorts of problems and the solutions that are able to attend to them, are also closely related to the problem / solution matrix relating to DeepFakes & Fraud.

Therein, there are a variety of ecosystem considerations that have been loosely considered in relation to furnishing means to consider these factors as part of the broader objective of seeking to support human dignity.

Psychological Attack & PsyOps

The purpose of psychological attacks; either directed at the victim or about the victim, is directed to support StrategicHarms usually for purposes relating to MisRepresentation and CommercialExploitation.

PsyOps is a term that relates to a field considered to be a form of 'trade craft', although not peaceful nor considered to be lawfully employed within the civilian domain, freely.

Fundamentally, the purpose is to engage in Manipulation in-order to mute FreedomOfThought and engender outcomes that support the objectives of the attackers. These activities are in-effect a form of activity that relates to DigitalSlavery.

Public Sector Wrong Doings

Chat GPT:

Public sector crimes are illegal or unethical activities that are committed by individuals or organisations working in the public sector, such as government departments or agencies, critical public sector entities like police or social security offices, or parliamentary offices.

Some examples of public sector crimes include:

- Corruption: This can include activities such as accepting or offering bribes, embezzling public funds, or using public office for personal gain.
- Fraud: This can include activities such as making false or misleading statements in order to obtain public funds or benefits, or using false or misleading information to obtain contracts or tenders.
- Misuse of public resources: This can include activities such as using public resources for personal gain or for activities that are not related to the official duties of the organisation.
- Insider trading: This can refer to the use of non-public information about a government agency or public sector entity to make trades or investments.
- Health and safety violations: This can include activities such as failing to provide a safe work environment or ignoring safety regulations, particularly in the context of critical public sector entities like police or social security offices.

Public sector crimes can have serious consequences for the individuals and organisations involved, as well as for society as a whole. They can undermine trust in public institutions and systems, damage reputations, and result in significant financial losses. It is important for public sector organisations and individuals to be aware of the risks of public sector crimes and to take steps to prevent and detect them, such as by implementing strong internal controls and compliance programs and training employees on ethical business practices.

Some other examples of public sector crimes include:

- Misuse of power: This can refer to the abuse of authority or position in order to gain an unfair advantage or to engage in activities that are not in the public interest.
- Discrimination: This can refer to the act of treating someone unfairly or unfairly denying them access to resources or opportunities based on their race, ethnicity, gender, sexual orientation, age, or other protected characteristic.
- Bribery: This can refer to the act of offering or accepting bribes in order to gain an unfair advantage or to influence the actions of a public sector entity or individual.
- Violation of privacy: This can refer to the unauthorised collection, use, or disclosure of personal information, particularly in the context of critical public sector entities like police or social security offices.
- Misuse of confidential information: This can refer to the unauthorised use or disclosure of confidential information, such as trade secrets or sensitive government documents.

Overall, public sector crimes can take many forms and can have serious consequences for the individuals and organisations involved, as well as for society as a whole. It is important for public sector organisations and individuals to be aware of the risks and to take steps to prevent and detect these types of crimes.

Define Malfeasance?

Malfeasance refers to the act of performing a legally or ethically wrong or improper act, particularly while in a position of trust or authority. It is often used in the context of public officials or employees who abuse their power or position for personal or financial gain, or to engage in activities that are not in the public interest.

Examples of malfeasance can include activities such as embezzlement, bribery, fraud, misuse of public resources, and abuse of power. Malfeasance can have serious consequences for both the individuals and organisations involved, as it can undermine trust in public institutions and systems and result in significant financial losses.

It is important for individuals and organisations to be aware of the risks of malfeasance and to take steps to prevent and detect it. This can include implementing strong internal controls and compliance programs, training employees on ethical business practices, and holding individuals accountable for their actions.

Questions re: Probity

Probity refers to the quality of being honest, upright, and morally correct. It is often used in the context of public officials or employees who are expected to adhere to high standards of integrity and ethical conduct in their roles.

Probity is an important concept in public life, as it is essential for maintaining trust in public institutions and systems. Public officials and employees who demonstrate probity are seen as trustworthy and reliable, and they are more likely to be respected and trusted by the public.

Probity can be demonstrated through a number of behaviours, such as honesty, transparency, fairness, and accountability. It is important for individuals and organisations to uphold high standards of probity in order to maintain public trust and confidence. This can involve implementing strong internal controls and compliance programs, training employees on ethical business practices, and holding individuals accountable for their actions.

The opposite of probity is impropriety, which refers to the act of behaving in an improper or unethical manner, particularly while in a position of trust or authority. Impropriety can take many forms, such as corruption, abuse of power, or engaging in activities that are not in the public interest.

Impropriety can have serious consequences for both the individuals and organisations involved, as it can undermine trust in public institutions and systems and result in significant financial losses. It is important for individuals and organisations to be aware of the risks of impropriety and to take steps to prevent and detect it, such as by implementing strong internal controls and compliance programs and training employees on ethical business practices.

What's it called if a person is sought to be compelled to not tell the truth and/or cover up wrong-doing that has previously occurred by one or more persons (ie: government employees) *who infer and/or suggest that the person will not be provided any further governmental assistance or be considered for any grants or forms of support, if they speak about something that government has done that has caused them harm and/or serious injury?*

If a person is sought to be compelled to not tell the truth and/or cover up wrongdoing that has previously occurred by one or more persons (e.g., government employees) who infer and/or suggest that the person will not be provided any further governmental assistance or be considered for any grants or forms of support if they speak about something that the government has done that has caused them harm and/or serious injury, this could be considered witness tampering.

Witness tampering is a crime that involves attempting to influence, intimidate, or coerce a witness in order to prevent them from telling the truth or to influence their testimony. It is often used to obstruct justice or to interfere with legal proceedings.

Witness tampering can take many forms, such as threatening or intimidating a witness, offering a witness a bribe or other inducement to not testify or to testify falsely, or withholding or destroying evidence. It is illegal and can result in criminal charges and severe penalties, including imprisonment and fines.

Overall, it is important for individuals and organisations to be aware of the risks of witness tampering and to take steps to prevent and detect it. This can include implementing strong internal controls and compliance programs, training employees on ethical business practices, and holding individuals accountable for their actions.

In addition to witness tampering, there are other terms that might be used to describe the sort of wrongdoing you described, such as:

- Obstruction of justice: This refers to the act of interfering with the administration of justice or the investigation or prosecution of a crime. It can include activities such as tampering with evidence, hindering an investigation, or influencing a witness.
- Bribery: This refers to the act of offering or accepting a bribe in order to influence the actions or decisions of another person. It can include activities such as offering a reward or inducement to a witness to not testify or to testify falsely.
- Intimidation: This refers to the act of threatening or coercing another person in order to influence their actions or decisions. It can include activities such as threatening a witness to not testify or to testify falsely.
- Fraud: This refers to the act of intentionally deceiving or misleading someone in order to gain an advantage or benefit. It can include activities such as making false or misleading statements to a witness in order to influence their testimony.

Overall, these types of wrongdoing can have serious consequences for both the individuals and organisations involved, as they can undermine trust in public institutions and systems and result in significant financial losses. It is important for individuals and organisations to be aware of the risks of these types of wrongdoing and to take steps to prevent and detect them. This can include implementing strong internal controls and compliance programs, training employees on ethical business practices, and holding individuals accountable for their actions.

TO BE CONTINUED...

The illustrated concept of a 'reversal', is about circumstances where a bad actor has knowingly engaged in activities that have harmed the target, and when questioned about it either makes claims about being the victim or otherwise seeks to isolate the target.

Some examples might be;

a group of people engaged in some form of CriminalActivity and they are fearful that a person who did not participate in those activities may be heard and that the outcome would be bad for that group of people. So, they seek to ensure that the person who was not involved in the wrong-doing is never able to be heard by anyone.

This in-turn relates also to Dehumanisation and other StrategicHarms, although generally also linked with CommercialExploitation and/or related motivations.

These sorts of SocialAttackVectors are difficult and usually non-trivial to triage; as such part of the mechanisms also relate to TemporalAttacks and objectives that seek to ensure that the costs of engendering some sort of bad outcome for wrong-doers is made to be as high as possible; therein, this is one of many tactical methods employed.

Social Contract Gamification

The concept of 'social contracts' is often used in connection to agreements that are made between people and/or between people and a named group of persons.

The concept of gamification, when applied to social contract concepts, through the lens of how the activity may be used to perform a social-attack, relates to an action or activity that involves at least 1 person intentionally producing a strategy that is intended to harm the target for whatever reason. This may be due to various types of SocialAttackVectors, yet the instigators do in-turn seek to engender an attack upon another person or persons; and others may in-turn become involved without being furnished an informed basis through which they are then in-turn made able to discern how and/or why they do so. This is in-turn also characteristic of a type of behaviour that is carried out online that has the effect of inducing Dehumanisation behaviours and breaches to the underlying FreedomOfThought SafetyProtocols requirements.

Not all problems are able to be canvassed in public. There are serious issues that relate to serious CriminalActivity that cannot be reasonably published online for all to employ as part of a gamification activity - notwithstanding the sense that some people appear to find personal gratification by engaging in activities that seek and/or successfully to do so. Thereafter harms upon one individual target may in-turn have negative and harmful impacts upon an array of persons that surround that individual, who the primary victim may seek to protect by ensuring the broader implications are unknown.

The most common method of social-contract gamification, is that a person with a higher-degree of influence and/or stature within a group; engages in a wrongful activity, and then goes about forming new documents and proclamations with the intended purpose of seeking to make it appear as though their target prosecuted behaviours that breached some form of reasonable moral standard; when in-fact, it was the attacker who breached those standards and perhaps also, any agreements or related instruments pertaining to the moral standards did not exist at the time of the event; which both provides a means through which the attacker, if found out, can claim that it didn't exist at the time so therefore they didn't break any agreements; but moreover the purposeful intent is to exact a TemporalAttacks upon their victim.

Various approaches and related tools that are sought to be produced to address these problems will be documented in the SafetyProtocols related considerations / notes.

Temporal Attacks

There are many different types of temporal attacks, one of the ones that makes me upset is the one that's about a person, often representing an entity (often an entity of public trust); that *'they're doing it all already'*.

The other is the one that's about a person who may be scouting for opportunities and in-order to diminish a person presenting the work that they've done (and any value or cost that may be attributed to that work); they focus on what hasn't been done, making the inference that nothing they've done is useful unless they continue to produce more work to produce more output; and this behaviour is in-turn cyclical, it doesn't actually matter how much work a person has done - the temporal attack is a form of abuse.

Other temporal attacks include;

1. Changing the content of an electronic record / document, to change the statements that were made earlier - without acknowledging that any changes were at all made.
2. Gamification; Often via groups of persons, a commercial attack that is intended to ensure the target is unable to do anything about a series of behaviours that intend to cause harm and/or immobilisation; in-order for the attacker to gain advantage and/or successfully achieve an outcome that was originally the work of the victim of this sort of attack, but is later misappropriated elsewhere - at which stage, there is no legal remedy that is able to resolve the harms caused to the victim of the attacks. These behaviours in-turn relate to obstruction and other issues relating to both civil and criminal matters of concern.
3. Removal of records; the deletion of evidence relating to wrong-doing for the purpose of making the claim that the wrong-doing was never done at all.
4. Versioning: whilst there's various forms of it, the underlying notion is that a group of people (often unpaid) start a body of work, which is later progressed by others who may be employed and their employers (or investors) see the merit of the works; then as future works are produced, they act to version-out the original creators, making it impossible to see the history of how something came about; and in-turn also, the relationships to whomever was involved at a time earlier to the commercialisation of derivatives from a project.

More to come.

NB: the underlying method to address this problem is via support for TemporalSemantics.

The Harvester

The concept of "The Harvester" refers to agents that engender others to do useful work that they seek to consume without any consideration about compensation or other forms of acknowledgement or more broadly, consideration.

Whilst the semantics for gaining knowledge implicitly relies upon socialisation, the mechanisms related to these sorts of 'harvester' attack vectors; often relate to Dishonesty, False Attribution and Commercial Exploitation which does in-turn negatively impact ESG whilst more broadly exposing those who have been mislead to various risks.

These sorts of behaviours are commonplace throughout both the public and private sectors. The ramifications negatively impact persons, particularly those involved in KnowledgeWork and leads to both DigitalSlavery related consequences, which may in-turn become associated with CriminalActivity and/or PublicSectorWrongDoings, which implicitly relies upon TheSecret and is fundamentally an act that is of a Dehumanisation nature.

Part of the underlying problem, which has seemingly not been considered a priority to resolve; is that there are various socio-economic models that have the effect of limiting the means through which those who may engage in these sorts of behaviours are provided a simple and easy to employ alternative. This is in-turn part of what is being addressed both via TheValuesProject and in-turn also, TheWorkPlatform.

"The Secret"

The concept of 'the secret' refers to circumstances where an allegation or statement is made by an agent in a manner that is not made known to the primary target of the statement; that is intended to elicit or invoke a behaviour that is harmful to the target and thereby/thereafter untrue or malignantly illustrated in a wrongful manner.

Issues related to this form of attack includes; Denial of Natural Justice, Torts and implications whereby persons may be co opted to support any other SocialAttackVectors in a manner that seeks to strategically ensure that the target is unaware of the problem and is therefore made incapable of being furnished means to address any such problem and the implications of any additional issues that may have been incurred as a consequence of these forms of attack vectors.

Whilst the semantics of who should be considered the primary target is a complex issue; as some may argue that the person being co opted is the primary target, whilst implicitly thereafter - the person that is sought to be maligned by "The Secret" is implicitly also the intended target. As such, the underlying series of events and related social mechanisms result in a 'graph' of events that result in many persons being harmed.

These sorts of attacks are also linked to the GuardianshipSemantics issues; as bad actors will often target persons who are not best equipped to make proper considerations about the nature of the event, that they are sought to take on - in good faith - as fact.

factors relating to TemporalAttacks (whilst not exclusively) are of great significance, as the consequence is often a circumstance where various effects of these behaviours render outcomes that may or may not have a means to render lawful remedy that is able to repair the harms that have been engendered. The effect of this consideration denotes the reality (physics and sociology, etc) whereby a person who is subjected to wrongs without available lawful remedy and/or ability to be afforded natural justice is obstructed and/or sought to be impaired and made inaccessible; the consequences may have impacts that can never be adequately responded to by compensation alone.

There is also an array of complex semantics relating to other temporal factors; which may include, circumstances where a false statement is made - but at the time, unclear, whereas over a period of time the nature of that situation may become clear and/or considered or made known (ie: courts of law, etc.) but that the false statements are maintained either or both in electronic systems that are sought to be lawfully relied upon and/or (interactively) via social agents more broadly. Therein, the culpability of those involved becomes greater overtime should the matter not be rendered with effect an ability to be triaged and resolved.

The effect of these sorts of problems often relates to Dehumanisation, CommercialExploitation and in-turn both CriminalActivity & PublicSectorWrongDoings.

A challenge in seeking to address this problem is that there are implications that invoke lawful responsibilities to be made tangibly employed by persons who may have traditionally done otherwise, as such, there are various implications of difficulty and thereafter also - significance; including but not limited to, considerations that are noted in relation to the topic of DigitalSlavery.

Complexities - Dignity / Privacy

Whilst it is too often the case that the concept of privacy is intentionally misused; as to, for instance, suggest that records about a person are unavailable to that person due to privacy considerations made by an offending entity...

There are other situations where matters of significance; including but not limited to the human rights of others, cannot be disclosed publicly as to support appropriate and proportionate support for providing remedy to any and all social wrongs / attack vector implications; that may disaffect the target of wrong-doings. Some examples are provided in the DigitalSlavery notes, yet others may relate to Mental Illness, GuardianshipRelations and/or professional obligations (ie: confidentiality duties) and various other forms of circumstances. The design challenge is therefore to seek to ensure that the methodologies that are employed are sensitive to these sorts of issues.

Torts

A tort is a civil wrong that causes a claimant to suffer loss or harm, resulting in legal liability for the person who commits a tortious act.1 Tort law can be contrasted with criminal law, which deals with criminal wrongs that are punishable by the state. While criminal law aims to punish individuals who commit crimes, tort law aims to compensate individuals who suffer harm as a result of the actions of others.2a Some wrongful acts, such as assault and battery, can result in both a civil lawsuit and a criminal prosecution in countries where the civil and criminal legal systems are separate. Tort law may also be contrasted with contract law, which provides civil remedies after breach of a duty that arises from a contract. Obligations in both tort and criminal law are more fundamental and are imposed regardless of whether the parties have a contract.

While tort law in civil law jurisdictions largely derives from Roman law, common law jurisdictions derive their tort law from customary English tort law. In civil law jurisdictions based on civil codes, both contractual and tortious or delictual liability is typically outlined in a civil code based on Roman Law principles. Tort law is referred to as the law of delict in Scots and Roman Dutch law, and resembles tort law in common law jurisdictions in that rules regarding civil liability are established primarily by precedent and theory rather than an exhaustive code. However, like other civil law jurisdictions, the underlying principles are drawn from Roman law. A handful of jurisdictions have codified a mixture of common and civil law jurisprudence either due to their colonial past (e.g. Québec, St Lucia, Mauritius) or due to influence from multiple legal traditions when their civil codes were drafted (e.g. Mainland China, the Philippines, and Thailand). Furthermore, Israel essentially codifies common law provisions on tort.

Outline of tort law

Source: Wikipedia

The following outline is provided as an overview of and introduction to tort law in common law jurisdictions:

Tort law – defines what a legal injury is and, therefore, whether a person may be held liable for an injury they have caused. Legal injuries are not limited to physical injuries. They may also include emotional, economic, or reputational injuries as well as violations of privacy, property, or constitutional rights.

Torts against the person

Torts (trespass) against the person – category of torts that describes a civil wrong that causes physical harm to the complainant:

- Assault (tort) – intentionally and voluntarily causing the reasonable apprehension of an immediate harmful or offensive contact.
- Battery (tort) – Bringing about an unconsented harmful or offensive contact with a person or to something closely associated with that person (such as an item of clothing). It differs from assault in that it requires actual contact.
- False imprisonment – A person is intentionally confined without legal authority.
- Intentional infliction of emotional distress – Intentional conduct that results in extreme emotional distress.

Negligent torts

Negligence – failure to exercise the care that a reasonably prudent person would exercise in like circumstances

- Breach of duty – There can be no liability in negligence unless the claimant establishes that he or she was owed a duty of care by the defendant and that there has been a breach of that duty.
- Legal causation or remoteness – The idea that liability may be so remote from the defendant that the negligence was not foreseeable or preventable by that party.
- Negligent Infliction of Emotional Distress - The idea that one has a legal duty to use reasonable care to avoid causing emotional distress to another individual.
- Malpractice or professional negligence – Negligence in the provision of a professional service causing harm to the claimant. Common varieties include medical malpractice and legal malpractice
- Negligence *per se* – Conduct which by its very nature gives rise to a presumption of negligence.

Property torts

- Trespass to land – Committed when an individual intentionally enters the land of another without lawful excuse. It is actionable *per se*, and thus the party whose land was entered may sue even if no actual harm is done.
- Trespass to chattels – Committed when an individual intentionally interferes with the personal property of another. Slight deprivation, like briefly placing a hand on someone else's car, is not actionable.
- Conversion (law) – An intentional tort to personal property where the defendant's willful interference with the chattel deprives the plaintiff of the possession of the same.
- Nuisance – Denial of quiet enjoyment to owners of real property. A private nuisance is an unreasonable, unwarranted, or unlawful interference with another person's private use and enjoyment of his or her property; whereas a public nuisance is an interference with the rights of the public generally. The test to determine whether an interference is reasonable is whether the gravity of the harm is outweighed by the social benefit of the nuisance.

Dignitary torts

Dignitary torts – a specific category of intentional torts where the cause of action is being subjected to certain kinds of indignities.

- Defamation – The communication of a statement that makes a false claim, expressly stated or implied to be factual, that may harm the reputation of an entity.
  - Libel – Written defamation
  - Slander – Spoken defamation
  - False light – A tort unique to American jurisprudence which covers defamatory statements which, although true, can give rise to false negative perceptions of the claimant.
- Invasion of privacy – The unlawful intrusion into the personal life of another person without just cause.
- Breach of confidence – Protects private information conveyed in confidence; typically requires that the information be of a confidential nature, communicated in confidence, and was disclosed to the detriment of the claimant.
- Abuse of process – A malicious and deliberate misuse or perversion of regularly issued court process not justified by the underlying legal action.

- Malicious prosecution – Similar to abuse of process, but includes intent, pursuing without probable cause, and dismissal in favour of the victim. In some jurisdictions, *malicious prosecution* is reserved for the wrongful initiation of criminal proceedings, while *malicious use of process* refers to the wrongful initiation of civil proceedings.
- Alienation of affections – Brought by a spouse against a third party, whom the spouse believes has interfered with his or her marriage. There is no requirement that all affections in the marriage be destroyed, only that there has been some diminution in the love and affection between the married couple.

Economic torts

Economic torts – torts that provide the common law rules on liability which arise out of business transactions such as interference with economic or business relationships and are likely to involve pure economic loss. Also called business torts.

- Fraud – Making of a false representation by one party with an intention to induce another party into an act of commission or omission owing to which the later party suffers a damage. The first Party may or may not benefit from the damage caused to the second party. Also, the first party need not be in collusion with someone who actually benefited.
- Tortious interference – One person intentionally damages the plaintiff's contractual or other business relationships.
- Conspiracy (civil) – An agreement between two or more parties to deprive a third party of legal rights or deceive a third party to obtain an illegal objective.
- Restraint of trade – Contractual obligations not to trade are illegal agreements on public policy grounds unless they are reasonable in the interests concerning both parties and the public at large; this mainly affects post-termination restrictive covenants in employment contracts.
- Passing off – The tort of selling goods or services in a manner that falsely causes customers to believe they originate from a different brand or supplier.

Strict and absolute liability torts

Further information: Strict liability and Absolute liability

- Product liability – The area of law in which products manufacturers, distributors and sellers are held responsible for the injuries caused by their products. Generally, a product liability claim is based on either a design defect, a manufacturing defect, or a failure to warn. This topic is closely associated with negligence, breach of warranty and consumer protection.
- Ultrahazardous activity – An activity so dangerous that a person engaged in such an activity can be held strictly liable for injuries caused to another person, regardless of whether or not reasonable precautions were taken to prevent others from being injured.
- Absolute liability – The rule in M. C. Mehta v. Union of India, in Indian tort law is a unique outgrowth of the doctrine of strict liability for ultrahazardous activities. Under this principle of absolute liability, an enterprise is absolutely liable without exceptions to compensate everyone affected by any accident resulting from the operation of hazardous activity.[1]

Economic Torts

Economic torts typically involve commercial transactions, and include tortious interference with trade or contract, fraud, injurious falsehood, and negligent misrepresentation. Negligent misrepresentation torts are distinct from contractual cases involving misrepresentation in that there is no privity of contract; these torts are likely to involve pure economic loss which has been less-commonly recoverable in tort. One criterion for determining whether economic loss is recoverable is the "foreseeability" doctrine.35 The economic loss rule is highly confusing and inconsistently applied36 and began in 1965 from a California case involving strict liability for product defects; in 1986, the U.S. Supreme Court adopted the doctrine in *East River S.S. Corp. v. Transamerica Deleval, Inc*.37 In 2010, the supreme court of the U.S. state of Washington replaced the economic loss doctrine with an "independent duty doctrine".38

Economic antitrust torts have been somewhat submerged by modern competition law. However, in the United States, private parties are permitted in certain circumstances to sue for anticompetitive practices, including under federal or state statutes or on the basis of common law tortious interference, which may be based upon the Restatement (Second) of Torts §766.39

Negligent misrepresentation as tort where no contractual privity exists was disallowed in England by *Derry v Peek* [1889]; however, this position was overturned in *Hedley Byrne v Heller* in 1964 so that such actions were allowed if a "special relationship" existed between the plaintiff and defendant.40 United States courts and scholars "paid lip-service" to *Derry*; however, scholars such as William Prosser argued that it was misinterpreted by English courts.40 The case of *Ultramares Corporation v. Touche* (1932) limited the liability of an auditor to known identified beneficiaries of the audit and this rule was widely applied in the United States until the 1960s.40 The Restatement (Second) of Torts expanded liability to "foreseeable" users rather than specifically identified "foreseen" users of the information, dramatically expanding liability and affecting professionals such as accountants, architects, attorneys, and surveyors.40 As of 1989, most U.S. jurisdictions follow either the *Ultramares* approach or the Restatement approach.40

The tort of deceit for inducement into a contract is a tort in English law, but in practice has been replaced by actions under Misrepresentation Act 1967.41 In the United States, similar torts existed but have become superseded to some degree by contract law and the pure economic loss rule.42 Historically (and to some degree today), fraudulent (but not negligent42) misrepresentation involving damages for economic loss may be awarded under the "benefit-of-the-bargain" rule (damages identical to expectation damages in contracts42) which awards the plaintiff the difference between the value represented and the actual value.42 Beginning with *Stiles v. White* (1846) in Massachusetts, this rule spread across the country as a majority rule with the "out-of-pocket damages" rule as a minority rule.42 Although the damages under the "benefit-of-the-bargain" are described as compensatory, the plaintiff is left better off than before the transaction.42 Since the economic loss rule would eliminate these benefits if applied strictly, there is an exception to allow the misrepresentation tort if not related to a contract.42

Intentional Torts

Source: Wikipedia.

Intentional torts are any intentional acts that are reasonably foreseeable to cause harm to an individual, and that do so. Intentional torts have several subcategories:

- Torts against the person include assault, battery, false imprisonment, intentional infliction of emotional distress, and fraud, although the latter is also an economic tort.
- Property torts involve any intentional interference with the property rights of the claimant (plaintiff). Those commonly recognised include trespass to land, trespass to chattels (personal property), and conversion.
- Dignitary torts are a category of intentional tort affecting the honour, dignity, and reputation of an individual and include: Defamation[k], invasion of privacy, breach of confidence, torts related to the justice system such as malicious prosecution and abuse of process, and torts pertaining to sexual relations that are considered obsolete in most common law jurisdictions such as alienation of affection and criminal conversation.

An intentional tort requires an overt act, some form of intent, and causation. In most cases, transferred intent, which occurs when the defendant intends to injure an individual but actually ends up injuring another individual, will satisfy the intent requirement.[31] Causation can be satisfied as long as the defendant was a substantial factor in causing the harm.

Negligence

Source - WikiPedia

The tort of negligence is a cause of action leading to relief designed to protect legal rights[g] from actions which, although unintentional, nevertheless cause some form of legal harm to the plaintiff. In order to win an action for negligence, a plaintiff must prove: duty, breach of duty, causation, scope of liability, and damages. Further, a defendant may assert various defences to a plaintiff's case, including comparative fault and assumption of risk. Negligence is a tort which arises from the breach of the duty of care owed by one person to another from the perspective of a reasonable person. Although credited as appearing in the United States in *Brown v. Kendall*, the later Scottish case of *Donoghue v Stevenson* [1932] AC 562, followed in England, brought England into line with the United States and established the 'tort of negligence' as opposed to negligence as a component in specific actions.[24] In *Donoghue*, Mrs. Donoghue drank from an opaque bottle containing a decomposed snail and claimed that it had made her ill. She could not sue Mr. Stevenson for damages for breach of contract and instead sued for negligence. The majority determined that the definition of negligence can be divided into four component parts that the plaintiff must prove to establish negligence.

In most common law jurisdictions, there are four elements to a negligence action:[25]

1. duty: the defendant has a duty to others, including the plaintiff, to exercise reasonable care[h]
2. breach: the defendant breaches that duty through an act or culpable omission
3. damages: as a result of that act or omission, the plaintiff suffers an injury

4. causation: the injury to the plaintiff is a reasonably foreseeable[i] consequence of the defendant's act or omission under the proximate cause doctrine.[j]

Some jurisdictions narrow the definition down to three elements: duty, breach and proximity caused harm.[30] Some jurisdictions recognize five elements, duty, breach, actual cause, proximate cause, and damages.[30] However, at their heart, the various definitions of what constitutes negligent conduct are very similar. Depending on jurisdiction, product liability cases such as those involving warranties may be considered negligence actions or fall under a separate category of strict liability torts. Similarly, cases involving environmental or consumer health torts which other countries treat as negligence or strict liability torts are treated in India as absolute liability torts.

In establishing whether a duty of care exists, different common law jurisdictions have developed a variety of distinct but related approaches, with many jurisdictions building on the test established in *Anns v Merton LBC*. In Singapore, the current leading case is *Spandeck Engineering v Defence Science and Technology Agency*, which builds on *Anns* by establishing a two step test comprising an analysis of proximate cause and public policy as a universal test, independent from the individual circumstances of a given case, for determining the existence of a duty of care. The Supreme Court of Canada established a similar test in the context of assessing damages for pure economic loss owing to negligence derived from *Anns* which consists of a two step examination of the existence of a sufficiently proximate relationship between the parties and public policy considerations; however, the Canadian test is more sensitive to the individual circumstances of a given case and the first step is generally deemed to be met where a case falls into one of three sets of circumstances recognised by precedent while the Singaporean test is independent of precedent. In English tort law, *Caparo Industries plc v Dickman* established a tripartite test for the existence of a duty of care per which harm must be reasonably foreseeable as a potential result of the defendant's conduct; the parties must be in a relationship of proximity; and it must be fair, just, and reasonable to impose such a duty.

Nuisance

Source: Wikipedia

"Nuisance" is traditionally used to describe an activity which is harmful or annoying to others such as indecent conduct or a rubbish heap. Nuisances either affect private individuals (private nuisance) or the general public (public nuisance). The claimant can sue for most acts that interfere with their use and enjoyment of their land. In English law, whether activity was an illegal nuisance depended upon the area and whether the activity was "for the benefit of the commonwealth", with richer areas subject to a greater expectation of cleanliness and quiet.[32] The case *Jones v Powell* (1629) provides an early example, in which a person's professional papers were damaged by the vapours of a neighbouring brewery. Although the outcome of this case is unclear,[32] Whitelocke of the Court of the King's Bench is recorded as saying that since the water supply in area was already contaminated, the nuisance was not actionable as it is "better that they should be spoiled than that the commonwealth stand in need of good liquor".[*citation needed*]

In English law, a related category of tort liability was created in the case of *Rylands v Fletcher* (1868): strict liability was established for a dangerous escape of some hazard, including water, fire, or animals as long as the cause was not remote. In *Cambridge Water Co Ltd v Eastern Counties Leather plc* (1994), chemicals from a factory seeped through a floor into the water table, contaminating East Anglia's water reservoirs.[33] The *Rylands* rule remains in use in England and Wales. In Australian law, it has been merged into negligence.[34]

Criminal Activity

Summary

Most Social Attack Vectors actually relate to the performance of criminal activities.

Here are some examples;

- CorporateCrime
- CyberCrime
- FinancialCrimes
- Fraud

and whilst the activity may or may not necessarily be criminal in nature or consequence, the underlying experience i've been made very much aware of; is the consequential ability for persons to thereafter be rendered gainful support via PublicSectorWrongDoings that can have the effect of all parties involved somewhat jointly seeking to ensure lawful remedy is not made available to the victim of any such forms of attacks, regardless of the consequences put upon that person and/or others relating to them. These sorts of problems are in-fact very serious and need to be addressed as a matter of priority; particularly, in relation to behaviours that have serious negative implications and/or impacts upon children, and particularly therein - those that relate to the behaviours of adults that target children.

ChatGPT:

In order for a person to be found guilty of committing a crime, the prosecution must be able to prove beyond a reasonable doubt that the person committed the crime as defined by law. This typically requires the prosecution to present evidence that demonstrates the elements of the crime, such as the act or conduct that constituted the crime, the intent or state of mind of the accused, and any attendant circumstances.

In criminal cases, the burden of proof is on the prosecution, and the accused is presumed innocent until proven guilty. This means that the prosecution must present evidence that is sufficient to overcome the presumption of innocence and to persuade the jury or judge that the accused is guilty beyond a reasonable doubt.

If the prosecution is able to meet this burden of proof, the accused may be found guilty of the crime. If the prosecution is unable to meet this burden of proof, the accused may be found not guilty or the case may be dismissed.

Overall, the legal standard for finding someone guilty of a crime is high, and it is designed to ensure that individuals are not wrongfully convicted of crimes they did not commit.

There are several procedural requirements that must be followed in order to address an issue of criminal wrongdoing online, particularly if the account being used is not easily associated with the legal person using it. Some of the key steps that may be involved in this process include:

1. Investigation: The first step in addressing an issue of criminal wrongdoing online is typically to conduct an investigation. This may involve collecting and analysing evidence, such as electronic records and documents, to determine the nature and extent of the wrongdoing.
2. Identification of suspects: If the investigation reveals that a crime has been committed, the next step is typically to identify the suspects involved. This may involve using forensic techniques to trace the IP address of the account being used or to identify any other identifying information that may be associated with the account.
3. Arrest and charging: If the suspects are identified and there is sufficient evidence to support charges, the next step is typically to arrest the suspects and charge them with the appropriate crimes.
4. Pre-trial proceedings: Once the suspects have been charged, the case will typically proceed to pre-trial proceedings, which may include plea negotiations, motions, and other legal proceedings.
5. Trial: If the case is not resolved through pre-trial proceedings, it will typically proceed to trial, where the prosecution will present its case and the defence will present its case.
6. Verdict and sentencing: If the suspects are found guilty, the court will typically impose a sentence, which may include imprisonment, fines, or other penalties.

Overall, the process of addressing an issue of criminal wrongdoing online can be complex and time-consuming, and it requires the involvement of law enforcement agencies and legal professionals. It is important for individuals and organisations to be aware of the risks of criminal activity online and to take steps to prevent and detect it.

Corporate Crime

Chat AI:

Corporate crime refers to illegal or unethical activities that are committed by a business or corporation. These crimes can take many forms and can involve one or more parties who are engaged in activities that breach laws or duties as described by corporate governance and related laws.

Some common types of corporate crime include:

- Financial crime: This can include activities such as embezzlement, money laundering, and securities fraud.

- Environmental crime: This can include activities such as illegal dumping of hazardous waste or violation of environmental regulations.
- Consumer fraud: This can include activities such as false advertising or selling defective products.
- Bribery and corruption: This can include activities such as offering or accepting bribes in order to gain an unfair advantage.
- Health and safety violations: This can include activities such as failing to provide a safe work environment or ignoring safety regulations.

Corporate crime can have serious consequences for both the businesses and individuals involved, as well as for society as a whole. It can undermine trust in businesses and financial systems, damage reputations, and result in significant financial losses. It is important for businesses and individuals to be aware of the risks of corporate crime and to take steps to prevent and detect it. This can include implementing strong internal controls and compliance programs and training employees on ethical business practices.

Some other examples of corporate crimes include:

- Intellectual property violations: This can include activities such as copyright infringement, patent infringement, and trademark infringement.
- Insider trading: This refers to the act of using non-public information about a company or financial instrument to make trades or investments. It is illegal because it gives an unfair advantage to the person with access to the insider information.
- Price fixing: This involves colluding with competitors to set prices at an artificially high or low level, in order to gain an unfair advantage in the market.
- Antitrust violations: This refers to activities that violate antitrust laws, which are designed to promote competition and prevent monopolies. Examples include price fixing, bid rigging, and market allocation.
- Fraud: This refers to the act of intentionally deceiving or misleading someone in order to gain an advantage or benefit. It can take many forms, including financial fraud, identity fraud, and fraudulent misrepresentation.

Overall, corporate crime can take many forms and can have serious consequences for both the businesses and individuals involved, as well as for society as a whole. It is important for businesses and individuals to be aware of the risks and to take steps to prevent and detect them.

Environmental Crime

This can include activities such as illegal dumping of hazardous waste or violation of environmental regulations.

Financial Crimes

OpenAI:

Financial crimes are illegal activities that involve the misuse or manipulation of financial systems or instruments for personal or financial gain. They can take many forms, including fraud, money laundering, and embezzlement.

Fraud refers to the act of intentionally deceiving or misleading someone in order to gain an advantage or benefit. It can take many forms, including financial fraud, identity fraud, and fraudulent misrepresentation.

Money laundering refers to the act of disguising the proceeds of illegal activities as legitimate funds. This is often done by transferring the funds through multiple transactions or accounts in order to obscure their origin and make it difficult to trace the money back to its source.

Embezzlement refers to the act of misusing funds or assets that have been entrusted to someone's care. This can include activities such as stealing money from an employer or organisation, or misusing company funds for personal gain.

Financial crimes can have serious consequences for both the individuals who commit them and the victims. They can undermine trust in financial systems, damage reputations, and result in significant financial losses. It is important for individuals and organisations to be aware of the risks of financial crimes and to take steps to protect themselves from them.

Other common types of financial crimes include:

- Insider trading: This refers to the act of using non-public information about a company or financial instrument to make trades or investments. It is illegal because it gives an unfair advantage to the person with access to the insider information.
- Ponzi schemes: This refers to a fraudulent investment scheme in which earlier investors are paid returns with the money of newer investors, rather than with actual profits. The scheme relies on the continuous recruitment of new investors to generate returns for earlier investors, and it eventually collapses when there are not enough new investors to pay off earlier investors.
- Cybercrime: This refers to criminal activities that involve the use of computers, networks, or the internet to commit crimes. Examples include computer hacking, online identity theft, and phishing scams.
- Securities fraud: This refers to the act of manipulating the stock market or securities in order to defraud investors. It can take many forms, including insider trading, misstating financial information, and manipulating the price of securities.

Overall, financial crimes are illegal activities that involve the misuse or manipulation of financial systems or instruments for personal or financial gain. They can have serious consequences for both the individuals who commit them and the victims, and it is important for individuals and organisations to be aware of the risks and to take steps to protect themselves from them.

Fraud

Open AI:

Fraud is the act of intentionally deceiving or misleading someone in order to gain an advantage or benefit. It can take many forms, including financial fraud, identity fraud, and fraudulent misrepresentation.

Financial fraud refers to the act of using false or misleading information to obtain money or other financial benefits. This can include activities such as embezzlement, counterfeiting, and identity theft.

Identity fraud refers to the act of using someone else's personal information, such as their name, address, or social security number, to obtain goods or services or to commit financial fraud.

Fraudulent misrepresentation refers to the act of making false or misleading statements in order to induce someone to enter into a contract or agreement.

Fraud is a serious crime, and it can have significant consequences for both the individuals who commit it and the victims. It is important for individuals to be aware of the risks of fraud and to take steps to protect themselves from it, such as by being cautious about providing personal information or by being vigilant for signs of fraudulent activity.

Proxy Attacks

The concept of 'Proxy Attacks' or 'attacks by proxy' is intended to refer to circumstances where an underlying attacker / bad actor; has enrolled others to perform an attack upon an intended victim, thereby seeking to remain undiscovered / secretly unable to be discovered and/or associated with the attack that is performed upon a target.

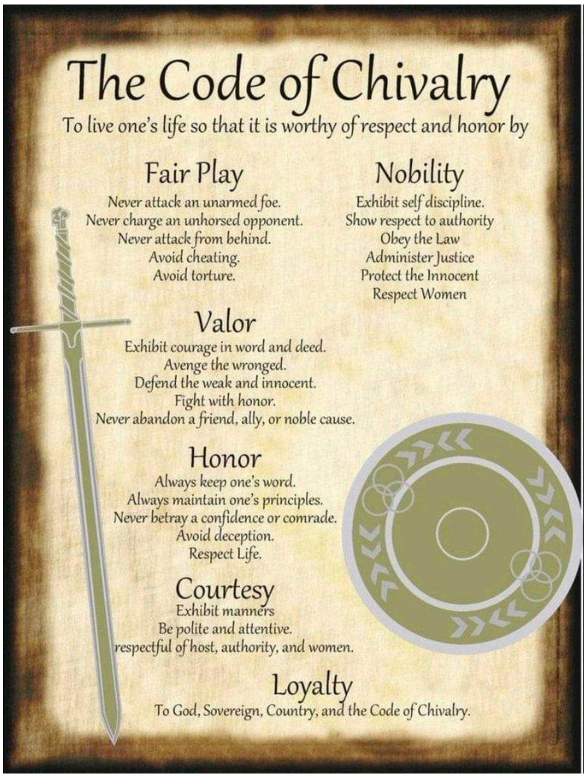
These sorts of attacks may incorporate various other activities that relate to persons knowingly involved in wrong-doing / crimes - whilst the actual attacker (the person committing the assaults) may not be aware of the implications or circumstances of importance relating to the pretext of having been employed to commit an attack upon the target.

In the worst types of situations; these sorts of attacks can have a meaningful relationship to issues otherwise noted in the DigitalSlavery considerations, alongside those associated with PublicSectorWrongDoings, notwithstanding broader associations with CommercialExploitation, CriminalActivity, AttacksOnline and other CyberAttackVectors, TemporalAttacks, Torts, Dehumanisation and just about anything else you can think of...

In-order to address the 'proxy attack' vectors; there needs to be a complex Human Centric AI Graph, that enables means for a court of law to lawfully seek information about the provenance of circumstances relating to harms that have been committed upon a person.

As far as I can recall, I am not aware of any situation where these sorts of methods have been employed that do not relate to the underlying actors seeking gainful outcomes, generally in relation to activities that seek to obtain or protect financial gains. In the most sophisticated examples; it is comparatively 'cheap' to make use of a small percentage of a large profit associated with wrongful gains; which when associated with 'deals' that yield more than a million dollars of profit (noting - the sophistication gets more complex when the gainful value is beyond $50m - $200m+); enables a person who presents with wealth, to encourage unsophisticated others to perform attacks whilst they're provided thousands and often a great deal more, via sophisticated schemes (often involving many public/private entities) to provide benefits that those people would never otherwise obtain; and, most often also - they're not actually aware of what it is that they've done, or the gainful outcome of it obtained by other persons. Therein also - often they're subjected to blackmail and other threats of consequences if they ever do anything that would act to deconstruct the proxy attack method (as to expose the underlying actors).

Part of the consequence of these attacks becomes; that WHEN the attacker and any people who supported acts of wrong-doing find out that they've engaged in wrongful behaviour, they're compromised and thereafter aligned with the values framework of the underlying attacker - which thereafter, becomes part of the broader DigitalSlavery and Dehumanisation issues that are related to CorporateCrime in particular, although not exclusively.



The Code of Chivalry

To live one's life so that it is worthy of respect and honor by

Fair Play

Never attack an unarmed foe.
Never charge an unhorsed opponent.
Never attack from behind.
Avoid cheating.
Avoid torture.

Nobility

Exhibit self discipline.
Show respect to authority
Obey the Law
Administer Justice
Protect the Innocent
Respect Women

Valor

Exhibit courage in word and deed.
Avenge the wronged.
Defend the weak and innocent.
Fight with honor.
Never abandon a friend, ally, or noble cause.

Honor

Always keep one's word.
Always maintain one's principles.
Never betray a confidence or comrade.
Avoid deception.
Respect Life.

Courtesy

Exhibit manners
Be polite and attentive.
respectful of host, authority, and women.

Loyalty

To God, Sovereign, Country, and the Code of Chivalry.

Safety Protocols

Made available as a google-doc for the purpose of encouraging participatory improvement on the 1st of March 2023. This document was originally intended / drafted, as part of the work on a form of implementation for Human Centric AI systems. As such, there may be specific qualities / design considerations, that are both draft and more broadly, not 'fit for purpose' for this broader series of considerations with respect to forming digital justice and social security systems. The elements need to be updated / re-drafted, to reflect upon the applied use of the prior draft texts; which has not yet been done.

This document has been generated from the content that was originally produced and published online via github into a documentation site.

The intended purpose of this document is to support the means through which safety protocols may be defined for use in human centric AI systems, namely the Human Centric AIsystems; although others are encouraged to produce fit for purpose solutions also, as to address the problems that are described by the document and related resources associated to what is defined as Social Attack Vectors.

The derivative solutions that are thought to address these and other social attack vectors, are sought to be defined as 'safety protocols' which incorporate technical, legal, social and other ecosystem components as to bring-to-effect, the means to significantly reduce harms; and improve accountability and/or presentation of complex issues and related facts, to courts of law; whilst protecting / preserving privacy and other related human rights that may otherwise not be able to be protected due to ICT systems Designs.

This document will also incorporate an array of other considerations that relate to the practical requirements that are considered likely necessary, in-order to ensure best-efforts are made to deliver technology ecosystem solutions that can give-effect to the delivery of safety protocols via technology.

Background: Introduction

There is a balance between absolute security and secrecy / privacy vs. social needs, to uphold basic values. The method considered most feasible to address this difficult balance, is embodied by the concept of creating Safety protocols.

The Safety Protocols requirement will end-up being defined in-full to be interoperable terms with The Declaration / Charter terms and statements, which are being developed in this document.

The Effect of developing 'safety protocols' is instrumental to providing a means to develop a decentralised social-web framework that supports values based networking between agents (people) in a way that supports the recognition and use of declared values, to provide support for agents to provide the necessary social protections needed, to be able to create safe decentralised online environments.

To the greatest capacity available; the intention is to make as many of the safety protocols as possible, optional. However, the idea is that there will be notifications about whether or not another agent is running a particular type of safety protocol; as to alert others to their status or ideology, and thereby provide an ability for others they are communicating with, to decide how and/or if they want to communicate with that agent, by being able to take into account whether and/or what safety protocols they're operating.

Safety protocols may relate to providing insights as to whether or not an agent is who they claim themselves to be; or whether they've got particular protocols that are operated in-order to protect themselves and others from materials that are blatantly criminal and/or relating to abuses of the human rights of others.

Safety protocols can be employed at different levels; some will be designed to operate at the systems level, others will be designed to operate in connection to the functionality of an app.

Safety protocols will employ ValuesCredentials and PermissiveCommonsTech, alongside other tooling as required to make an environment that is both able to be made highly secure, and simultaneously also - support safety both for the user and others they interact with, based upon the values they decide to be important for themselves, as individuals / groups.

When defining Human Centric AI- I want to consider the various ways through which values have been expressed overtime, by persons and groups from various places throughout the world, overtime.

One example is the The Code of Chivalry, as illustrated earlier, others are embodied by the 'values credentials' and related instruments; and others yet, include such things as The Three Laws of Robotics; As was first published in 1942 by Isaac Asimov , the concept therefore pre-dates the 1945 post war article by Vannaver Bush on 'As We May Think'.

First Law:

A robot may not injure a human being or, through inaction, allow a human being to come to harm.

Second Law:

A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.

Third Law:

A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

What other Rules need to be defined?

Considerations include;

1. It has an owner: it serves its owner(s).
2. They probably need to be defined in a way that supports the ability for a family to have many different Human Centric AIrunning on the same 'Human Centric AIbox'; but if there's a change (family separation, or child becomes an adult) their 'webizen' can be migrated.
3. If the owner is a child or is otherwise similarly incapable of 'personhood', then it shall be subject to the rules defined by that person's guardian & the 'Human Centric AIrules'.
4. Cannot Fabricate 'evidence', that there must be an ability to audit the logical basis of bot facts
5. Defining the rules of 'Battle Bots'; what is allowed in the civilian domain and what is not allowed?
6. How are rules defined to ensure the people, Human Centric AIserve are protected from acts of violence, harms, threats, etc..

Human Centric AIEthics (cont).

There are also significant ideological considerations that do need to be made; about the difference between designing a 'thing' that is a tool; and that the responsibility over how it is designed to operate by its owner, is really up to that person - which is in-turn, a morality related method; that seeks to support 'personal responsibility' rather than 'big brother' or 'system defined rules' of conduct. This methodology; is in-turn, a bit like providing other types of tools, whether it be desktop computers or applications that work on them, like spreadsheet programs; or physical artefacts, like cars or hammers; all of which, can be used for harmful / wrongful purposes; But that there's either no controls, or limited controls placed upon the sale of these 'products'.

In effect a design method; to support the notion, that "The primary person responsible for one's behaviour is themselves…"... Therein - design standards would in-turn seek to ensure that the natural persons who own their 'Human Centric AI Agent' (environment); is supported, in seeking to ensure that they are indeed, responsible for the actions of their webizen. This would include an array of design qualities & requirements; to ensure this form of ideology is indeed supported; whilst also offering a capacity for innovators to innovate.

But the consequence, much like cars or hammers - is that people might seek to use them as a weapon; as such, there are various considerations to be made about how best to address this problem, perhaps not so much in relation to the 'webizen' tooling itself; but moreover, how it is designed to be supported by broader ecosystems - including but not limited to, law & legal processes.

Yet - these considerations are not intended to entirely absolve responsibility for ensuring good design. Part of the 'webizen.org' initiative, is to figure out how to form a multi-stakeholder approach to forming 'open standards' that support and are in-turn supported by participants who get involved.

There are various methods to seek to provide hygiene and ensure that 'Human Centric AI systems' are safe and indeed also; very secure (technically).

It is considered that a 'webizen' be a far more complicated form of 'identity apparatus' or tooling; which is very different to the present-day mainstream 'beliefs' about the benefits for mankind by issuing them 'wallets' powered by 'web3' with keys / credentials, that can be reissued in the case the wallet is lost.

This isn't just about 'wallets', its moreover about human agency - and the need to produce a solution, despite the consequences of decisions made by others to not provide infrastructure online to support human agency (ie: my old 'knowledge banking' works); by refactoring the designs, to better consider / take into account; the circumstances where the primary goals relate to 'property' (inclusive to AI / Information Infrastructure) & contract law.

The outcome of producing Webizen, should result in significant 'safety / dignity' improvements for the people who are able to buy one, and have it help them with their life as influenced by technology. Part of how this will be achieved is via 'safety protocols' (per below, but think - star-trek, holodeck - which has safety protocols); therein, some of what needs to be done, is a bunch of work on various forms of values frameworks that need to be produced as ontologies, so that owners can decide which 'optional' ones they want to employ' whilst, the product may not function if the mandatory ones are not 'turned on' or in some way otherwise corrupted (aka safety protocols).

Necessary Protections - SafetyProtocols

In Star-Trek Voyager - the 'holodeck' systems, have 'safety protocols' to protect people; so should webizen. Designing these systems is important, so that the way those safety outcomes are achieved; are designed, rather than forced - in ways that are likely to result in other sorts of consequences.

Whilst I'm not sure what they will be yet, there is a need to ensure these boxes cannot be used in a federated manner to engender an attack..

The types of attacks will need to be defined (mis-use cases; and in-turn, a framework to attend to these threats developed and addressed; in a manner that does not breach ‘first principles’ which are in-turn also to be defined, but are essentially about the protection and support of human rights.

These ‘codes’ should be produced as part of the webizen.org works broadly; leveraging, broad-ranging discussions about ‘ai ethics’ through a different lens; a lens, where its now able to be focused upon a concept where, people, may in-future, own their own robots; and as a new and innovative form of ‘artificial species’ or ‘artificial agent’, form ‘common-sense’ approaches to what sorts of things should be discouraged, what sorts of governance principles should apply - and fundamentally; when a person gets a ‘webizen’, perhaps they sign an oath; or, that they’ll need to install their own software/firmware, as a consequence of deciding not to; but, part of the necessary protections are also, that people should be able to transfer their Human Centric AI environments (the data / software environment) and operate it on compatible systems; as is a form of protection.

#socialfabric #ValuesFrameworks #SafetyProtocols

Agent Labelling

It is important that there is a clear means to distinguish between the content, information or processes and decisions that are made by Software Agents (AI) Vs. those made by legal entities; and in-turn also, the ability to determine which specific human beings were involved in many or causing any sort of causality related action to occur.

Asking ChatGPT;

My Question: What are the sorts of dangers, threats and social attack vectors that may occur if human beings are falsely led to believe they are consuming the work of other human beings or legal entities; when in-fact they're consuming information generated via an artificial intelligence software program?

ChatGPT Answer: *There are several dangers and threats that may occur if individuals are falsely led to believe that they are consuming information generated by other human beings or legal entities when it is actually generated by an artificial intelligence (AI) program. Some of these include:*

- Misinformation and disinformation: AI-generated content can be used to spread false or misleading information, which can have negative effects on individuals and society at large.

- Manipulation and influence: AI-generated content can be used to manipulate individuals and groups by appealing to their emotions, biases, and prejudices.
- Privacy and security concerns: AI-generated content can be used to target individuals with personalised phishing, scams, and other malicious attacks.
- Dehumanisation and mistrust: People being exposed to AI generated content that is falsely presented as being generated by human could lead to mistrust in human-generated content, leading towards a dehumanisation of human expression as well as a mistrust in human-generated content, AI-generated content can be used to perpetuate stereotypes and reinforce societal biases.
- Interfere with legal process: AI-generated content can be used to impersonate people or entities for fraudulent activities or illegal activities and could interfere with legal proceedings.

Overall, it is important for individuals to be able to distinguish between AI-generated content and human-generated content in order to make informed decisions and to protect themselves from potential dangers.

Another potential danger of falsely believing that information is generated by human beings when it is actually generated by AI is that it may lead to a lack of critical thinking and evaluation of the information being consumed. If people believe that the information they are consuming is coming from a trusted source, they may be less likely to fact-check or critically evaluate it. This can lead to the spread of misinformation and disinformation, as well as a decrease in people's ability to make well-informed decisions.

Additionally, there may be ethical concerns associated with the use of AI-generated content, particularly when it is used to impersonate human beings or legal entities. The ability to generate content that is indistinguishable from human-generated content raises questions about consent and accountability, as well as potential harms that may be caused by the use of this technology.

Finally, the widespread use of AI-generated content has the potential to disrupt various industries and change the way people think about and interact with information. It could change how professional authors, journalists, and creative professionals work, which could have both positive and negative impacts on the economy and society.

My Question: What are some of the threats related to circumstances where government departments and/or employees may use Artificial Intelligence to act in a manner that has human rights implications in relation to the effect of those actions if it is not clearly labelled to have been done via an AI Agent?

ChatGPT Answer:

If government departments or employees use Artificial Intelligence (AI) in a way that has human rights implications and it is not clearly labelled as having been done by an AI agent, there could be several threats. Some of these include:

- *Discrimination and bias: If an AI system is not transparent in its decision-making processes, it may perpetuate discrimination and bias against certain individuals or groups, potentially violating their human rights.*

- Lack of accountability: If an AI system is used to make decisions or take actions that have human rights implications, it can be difficult to hold individuals or organisations accountable if the system is not clearly labelled as an AI agent and its decision-making process is opaque.

- *Due process concerns: If an AI system is used to make decisions that affect an individual's rights or freedoms, it may not always provide the same level of due process protections as a human decision-maker. This could lead to violations of human rights and the rule of law.*
- *Privacy and security: If an AI system is used to process personal data without proper regulation or oversight, it could lead to privacy violations, security breaches, and other harms.*
- *Lack of transparency: If the actions of an AI agent is not clearly labelled, it can make it difficult for people to understand how decisions are being made, which could lead to mistrust and lack of transparency.*

- Interference with human autonomy: If an AI agent makes decisions that have significant impact on human life, people may lose their autonomy in the decision making process and their right to self-determination.

Overall, it is crucial that government departments and employees are transparent in their use of AI, clearly label any decisions or actions that are made by an AI agent, and ensure that the AI systems they use are fair, accountable, and respect human rights.

Another potential threat is that the AI may have unintended consequences on human rights, if it is not properly implemented, tested, and monitored. Even if the AI system is not inherently biassed, the data it is trained on may be biassed, leading to unjust outcomes.

Additionally, if the use of AI is not transparent and the decision-making processes of the AI system are not explainable, it may be difficult for people to understand how the decisions are being made and to challenge them if they believe that their human rights are being violated.

Moreover, if AI agents are used in law enforcement or security, without proper oversight or regulation, there could be a risk that the AI systems may be used to infringe on individuals' rights, such as freedom of speech and freedom of assembly, or to target certain groups based on their ethnicity, religion, or political beliefs.

It is important that the use of AI by government departments and employees is subject to proper regulation and oversight, so that human rights are protected and that the actions of the AI systems can be transparently tracked and audited.

Finally, It is crucial that the AI systems are continuously monitored and evaluated for their impacts on human rights and adjustments or replacements are made if necessary.

My Question: what are some of the potential risks in circumstances relating to foreign governments?

ChatGPT Answer:

There are several potential risks in circumstances related to foreign governments using AI:

- Cyber espionage: Foreign governments may use AI to conduct cyber espionage or cyberattacks against other countries, potentially stealing sensitive information or disrupting critical infrastructure.
- Misinformation and disinformation: Foreign governments may use AI-generated content to spread false or misleading information, with the intention of manipulating public opinion or undermining the credibility of other governments.
- Interference in domestic politics: Foreign governments may use AI to interfere in the domestic politics of other countries, with the goal of swaying elections or influencing policy decisions.
- Economic espionage: Foreign governments may use AI to gain an unfair advantage in international trade, by collecting business intelligence and targeting specific industries or companies.
- Military advantage: Foreign governments may use AI to enhance their military capabilities, potentially threatening the stability of regions and global security
- Human Rights abuse: AI technology has been used by some governments to track and control their citizens, violating their privacy and freedom. This technology can also be used to identify and monitor individuals based on their ethnicity, religion, or political beliefs, leading to further human rights violations.

Overall, the use of AI by foreign governments has the potential to destabilise international relations and threaten the security and sovereignty of other countries. It is important for governments to be aware of these risks and to take steps to protect against them, through international cooperation, regulation, and diplomacy.

Another potential risk is that foreign governments may use AI in a way that violates international law or human rights. For example, they may use AI-enabled surveillance to target political opponents, or use autonomous weapons to target civilians in warfare. These actions can have significant negative consequences on human rights and global security.

Moreover, the increasing use of AI in economic and technological fields may lead to a power imbalance between countries that have access to advanced AI technology and those that do not, leading to further economic and societal inequality.

Furthermore, if AI is not controlled and regulated properly, foreign governments may use it to violate international norms, such as economic sanctions or arms control agreements.

Lastly, foreign governments may also use AI to target individuals, companies or countries with cyber-attacks and disinformation campaigns for political, economic, or military gain.

To mitigate these risks, it is crucial for countries to work together through international organisations and agreements to establish norms and regulations for the responsible development and use of AI, as well as to cooperate on matters of cyber security, disinformation, and human rights.

My Question:

What are some of the ways AI content and/or software actions could be clearly labelled and associated with the legal entity involved and responsible for that AI content and/or software action, including both any legal personality (ie: government department, institution, corporation or business,) as well as the specific natural legal entities / individuals (human beings) who were instrumentally involved in enabling or rendering the applied use of AI for the particular artefact or event?

ChatGPT Answer;

There are several ways that AI content and/or software actions can be clearly labelled and associated with the legal entity responsible for them, including both the legal personality (e.g. government department, institution, corporation or business) and the specific natural legal entities/individuals who were involved in enabling or using the AI for the particular artefact or event. Some of these methods include:

- Digital Signatures: Using digital signatures to verify the authenticity of AI content or software actions, and to link them to the legal entity or individual responsible for them.
- Attribution Statements: Including an attribution statement in the AI content or software that identifies the legal entity or individual responsible for it.
- Watermarking: Watermarking AI content or software with unique identifiers that can be used to trace it back to the legal entity or individual responsible for it.
- Logging: Keeping detailed logs of who had access to and used the AI system, and what actions they took.
- Transparency Reports: Publishing transparency reports that provide information on the legal entities and individuals involved in the development and use of AI, as well as the system's decision-making processes and any human rights considerations.
- Certifications: Certifying the AI system by a third-party, that verifies that the system meets certain standards, such as fairness and transparency
- Source codes or system architecture: Making the source codes or system architecture of AI systems available for public inspection, in order for third parties to verify how the systems make decisions.
- Human oversight: Ensuring that AI systems are designed with human oversight and decision-making capabilities to make adjustments or corrections if necessary, and keeping records of those adjustments or corrections.

Overall, it is important to ensure that the AI system is clearly labelled and that the legal entity or individual responsible for the system is easily identifiable and can be held accountable for its actions. This can be achieved through a combination of technical and organisational measures, such as the ones listed above, which should be chosen according to the specific context and the potential impacts of the system.

Another way of clearly labelling AI content and/or software actions and associating them with the legal entity responsible for them, is by using blockchain technology, it can enable the creation of an immutable and transparent record of the origin and usage of the AI content or software. This can enable users to verify the authenticity of the content and trace it back to the legal entity or individual that created it, providing a tamper-proof record of the development and usage of the AI system.

Another approach to clearly identify the responsible entity is by using standard data labels, like the "metadata" of digital files, AI artefacts should also have standard labels that clearly identify the legal entity or individual responsible for them, such as the developer, creator, owner, or operator.

Additionally, governments could also play a role in promoting transparency and accountability of AI systems by implementing regulations and guidelines on the labelling of AI content and software actions, and enforcing penalties for non-compliance.

Finally, it is important to note that it is not just a technical problem but also a societal one, and that it requires a multi-stakeholder approach, which includes industry, civil society, and government, to develop a solution and to ensure that it is effectively implemented.

Another way of clearly labelling AI content and/or software actions is by using certification systems. These systems involve an independent third party, such as a regulatory agency or industry group, evaluating the AI system and verifying that it meets certain standards, such as transparency, fairness, and accountability. These certifications can be used to clearly label the AI system and to provide assurance to users that the system has been independently reviewed and found to be trustworthy.

Another way of clearly labelling AI content and/or software actions is by using explainable AI (XAI) techniques, these techniques allow the AI system to explain its decision-making process to users in a way that is easy for humans to understand. This can help users to trust the system and to understand how it makes decisions, and also make it easier for legal entities or individuals to be held accountable for the actions of the system.

Finally, it is important to educate the public about the importance of clearly labelling AI content and/or software actions and associating them with the legal entity responsible for them. This can help to increase awareness of the risks associated with AI and to promote responsible use of the technology.

In summary, there are many methods for clearly labelling AI content and/or software actions and associating them with the legal entity responsible for them, such as digital signatures, attribution statements, watermarking, logging, transparency reports, certifications, blockchain, standard data labels, explainable AI (XAI) and education. These methods can be used in combination to provide a comprehensive approach to transparency and accountability of AI systems.

My Question: How might an ontology using RDF and common vocabularies be defined to provide a means to deploy these sorts of solutions? Can you give me an example of an RDF OWL ontology?

An ontology using RDF and common vocabularies can provide a structured way to describe and represent information related to the legal entity responsible for AI content and/or software actions, as well as the actions themselves. RDF (Resource Description Framework) is a standard for modelling information on the web, and it provides a way to express the relationships between resources (e.g. documents, people, and concepts) using a graph-based structure.

A simple example of an RDF OWL (Web Ontology Language) ontology for describing AI content and software actions could include classes such as "AI system", "Legal entity", "Individual", "Action", and "Responsibility". Each class would have a set of properties that describe their characteristics and relationships, such as "name", "developer", "owner", "operator", "decision-making process" and "Standards met", respectively.

For example, the class "AI system" could have properties such as "name", "developer", "owner", "operator" and "decision-making process". The class "Legal entity" would have properties such as "name", "type" (e.g. government department, institution, corporation or business), "location", and "jurisdiction". The class "Individual" would have properties such as "name" and "role" (e.g. developer, owner, operator). The class "Action" would have properties such as "name", "date", "type" (e.g. decision, action) and "outcome". The class "Responsibility" would have properties such as "level" (e.g. primary, secondary, etc) and "entity" (e.g. legal entity, individual)

These classes and properties can be interconnected to describe complex relationships between AI systems, legal entities, individuals, and actions, and can be used to trace the origin and usage of AI content and software actions, and to establish accountability and transparency. The use of common vocabularies, such as schema.org and others, would help to standardise the representation of the information and make it more easily understandable and usable by different systems and applications.

It's worth noting that this is just a simple example and that a more comprehensive ontology would be more complex and take into account the specific context and use case. And that, the use of RDF and OWL enables the use of formal reasoning to infer new information from the ontology, which is particularly useful for the transparency and accountability of AI systems.

Additionally, using RDF and OWL to represent an ontology can enable the use of formal reasoning to infer new information from the ontology, this is particularly useful for transparency and accountability of AI systems. For example, by creating inferences rules in the ontology, you can automatically infer information about the legal entities, individuals and actions responsible for an AI system, based on the properties of the AI system.

Moreover, using RDF and OWL in this context can also enable the integration of the ontology with other systems, such as databases, document management systems and even other AI systems. This is particularly useful for creating transparency and accountability solutions, where information about AI systems, legal entities and individuals need to be shared and combined across different systems.

Another advantage of using RDF and OWL is that they can leverage the Linked Data ecosystem, which allows for easy data sharing and integration across different organisations and domains. This allows for more collaboration between different stakeholders, like industry, civil society and government, to help ensure the transparency and accountability of AI systems.

Finally, it is important to note that creating an ontology is just a first step, the ontology itself should be continuously updated, maintained, and evaluated to make sure it is still useful and useful, to address the complexity and dynamic nature of the field of AI.

My Question:

Can you write an example in notation3 syntax?

ChatGPT Answer:

Sure, here is an example of an RDF ontology written in Notation3 (N3) syntax to describe an AI system and its responsible legal entities and individuals:

```
@prefix ai: <http://example.com/ontology/ai#> .

@prefix foaf: <http://xmlns.com/foaf/0.1/> .

@prefix org: <http://www.w3.org/ns/org#> .


ai:MyAI a ai:AI;

    ai:name "My AI System";

    ai:developer [ a foaf:Person; foaf:name "John Doe" ];

    ai:owner [ a org:Organization; org:name "Acme Inc." ];

    ai:operator [ a foaf:Person; foaf:name "Jane Smith" ];

    ai:decision-makingProcess "Explainable AI using Decision Trees" .
```

In this example, the ontology defines a class "AI" (ai:AI) and an instance of that class "MyAI" (ai:MyAI), it also specifies that "MyAI" has a name "My AI System", a developer "John Doe" (foaf:Person), an owner "Acme Inc." (org:Organization), an operator "Jane Smith" (foaf:Person) and a decision-making process "Explainable AI using Decision Trees"

This ontology uses prefixes to simplify the URIs (ai:, foaf:, org:) used in the statements. The prefixes indicate that the URIs in the ontology are from the given namespace, so "ai:AI" refers to the URI "http://example.com/ontology/ai#AI".

Note that this is a simplified example, in real-world scenarios, the ontology would likely have more classes and properties and also, would relate to other ontologies to provide more context and meaning, such as time, location, standards met, etc.

Additionally, the ontology can include more classes and properties such as "Action", "Responsibility", "Jurisdiction", "Location", "Date", "Standards", "Certification" and "TransparencyReports" that describe the actions taken by the AI system, the level of responsibility of the legal entities and individuals, the jurisdiction, location, date of action, standards met, certifications achieved and transparency reports respectively.

Here's an example of how these classes and properties can be added to the ontology:

```
@prefix ai: <http://example.com/ontology/ai#> .

@prefix foaf: <http://xmlns.com/foaf/0.1/> .

@prefix org: <http://www.w3.org/ns/org#> .

@prefix xsd: <http://www.w3.org/2001/XMLSchema#> .
```

```
ai:MyAI a ai:AI;

    ai:name "My AI System";

    ai:developer [ a foaf:Person; foaf:name "John Doe" ];

    ai:owner [ a org:Organization; org:name "Acme Inc." ];

    ai:operator [ a foaf:Person; foaf:name "Jane Smith" ];

    ai:decision-makingProcess "Explainable AI using Decision Trees" ;

    ai:performedAction [ a ai:Action; ai:name "Decision Making";

    ai:outcome "Approve the loan";

    ai:date "2022-01-12T10:30:00Z"^^xsd:dateTime];

    ai:responsibility [ a ai:Responsibility;

    ai:level "Primary";

    ai:entity [a org:Organization; org:name "Acme Inc." ;

    ai:jurisdiction "US";

    ai:location "New York";

    ai:standardsMet "ISO/IEC 27001:2013";

    ai:certifications "ISO/IEC 27001:2013 certified";

    ai:transparencyReports <http://example.com/reports/myaisystem> .
```

This enhanced example illustrates how more information can be added to the ontology, such as the actions taken by the AI system, the outcome, the date of the action, the level of responsibility of the legal entities and individuals, the jurisdiction, location, the standards met, certifications achieved, and transparency reports.

It is worth noting that the example provided is not intended to be a complete or perfect ontology but is meant to give an idea of how RDF and OWL can be used to represent an ontology that would help with transparency and accountability of AI systems.

My Question:

Can you provide a more comprehensive example in json-ld?

ChatGPT Answer:

Sure, here is a more comprehensive example of an RDF ontology written in JSON-LD (JavaScript Object Notation for Linked Data) syntax to describe an AI system and its responsible legal entities and individuals:

```
{

    "@context": {

        "rdf": "http://www.w3.org/1999/02/22-rdf-syntax-ns#",
        "rdfs": "http://www.w3.org/2000/01/rdf-schema#",
        "xsd": "http://www.w3.org/2001/XMLSchema#",
        "foaf": "http://xmlns.com/foaf/0.1/",
        "org": "http://www.w3.org/ns/org#",
        "ai": "http://example.com/ontology/ai#",
        "name": "ai:name",
        "developer": {
            "@id": "ai:developer",
            "@type": "@id"
        },
        "owner": {
            "@id": "ai:owner",
            "@type": "@id"
        },

        "operator": {
            "@id": "ai:operator",
            "@type": "@id"
        },

        "decision-makingProcess": "ai:decision-makingProcess",
        "performedAction": {
            "@id": "ai:performedAction",
            "@type": "@id"
        },

        "outcome": "ai:outcome",
        "date": "ai:date",
        "responsibility": {
            "@id": "ai:responsibility",
            "@type": "@id"
        },

        "level": "ai:level",
        "entity": {
            "@id": "ai:entity",
            "@type": "@id"
        },

        "jurisdiction": "ai:jurisdiction",
        "location": "ai:location",
        "standardsMet": "ai:standardsMet",
        "certifications": "ai:certifications",
        "transparencyReports": {
            "@id": "ai:transparencyReports",
            "@type": "@id"
        }
    },

    "@id": "ai:MyAI",
    "@type": "ai:AI",
    "name": "My AI System",
    "developer": {
        "@id": "foaf:JohnDoe",
        "@type": "foaf:Person",
        "name": "John Doe"
    },

    "owner": {
        "@id": "org:AcmeInc",
        "@type": "org:Organization",
        "name": "Acme Inc."
    },

    "operator": {
        "@id": "foaf:JaneSmith",
        "@type": "foaf:Person",
        "name": "Jane Smith"
    },

    "decision-makingProcess": "Explainable AI using Decision Trees",
    "performedAction": {
        "@id": "ai:Action1",
        "@type": "ai:Action",
        "name": "Decision Making",
        "outcome": "Approve the loan",
        "date": "2022-01-12T10:30:00Z"
    },

    "responsibility": {
        "@id": "ai:responsibility1",
        "@type": "ai:Responsibility",
        "level": "Primary",
        "entity": {
            "@id": "org:AcmeInc",
            "@type": "org:Organization",
            "name": "Acme Inc."
        }
    },

    "jurisdiction": "US",
    "location": "New York",
    "standardsMet": "ISO/IEC 27001:2013",
    "certifications": "ISO/IEC 27001:2013 certified",
    "transparencyReports": "http://example.com/reports/myaisystem"
}
```

In this example, the ontology defines several classes, such as "AI" (ai:AI), "Action" (ai:Action), "Responsibility" (ai:Responsibility), "Person" (foaf:Person), and "Organization" (org:Organization), it also specifies that "MyAI" has a name, developer, owner, operator, decision-making process, performed actions, outcome, date, level of responsibility, and jurisdiction, location, standards met, certifications and transparency reports.

The context provided, maps the prefixes used in the ontology to the corresponding URIs, as well as provides data types and relationships between the different classes and properties. This is used to make the JSON-LD data more easily readable for both machines and humans. As before, it's important to note that this is just an example and that the ontology can be much more detailed, depending on the complexity and dynamic nature of the field of AI.

CONSIDERATIONS

Whilst the specific approach certainly requires a great deal more work and consideration, the merit of the underlying notion appears to be considered important even by ChatGPT.

I hope this explains enough of this underlying consideration as is sought to be sufficiently illustrated, as to be added to the ToDo list for informatics policies relating to the development of Human Centric AIsystems.

Freedom of Thought

Freedom of thought is the freedom of an individual to hold or consider a fact, opinion, or belief without interference or coercion. It is a fundamental human right that is protected by various national and international laws and agreements, including the Universal Declaration of Human Rights. Freedom of thought allows people to form and express their own beliefs and opinions, and to think and speak freely without fear of reprisal or punishment. It is an essential element of a free and democratic society, as it enables individuals to engage in critical thinking, debate, and the free exchange of ideas. Freedom of thought is often closely connected to other fundamental rights such as freedom of speech, freedom of religion, and freedom of the press.

There are a few key measures that are typically required to protect freedom of thought:

1. Legal protections: Freedom of thought is often protected by national and international laws and agreements that prohibit interference with an individual's right to hold and express their own beliefs and opinions.
2. Political will: Governments and other authorities must be committed to protecting freedom of thought and be willing to take action to defend it when it is threatened.
3. A robust civil society: A strong and active civil society, including media, NGOs, and other organisations, can help to promote and defend freedom of thought by advocating for the rights of individuals and holding authorities accountable.
4. An informed and educated public: An informed and educated public is more likely to support and defend freedom of thought, as they are better equipped to understand the importance of this right and to recognize when it is being threatened.
5. A culture of respect and tolerance: A culture that values diversity of thought and encourages respectful dialogue and debate can also help to protect freedom of thought.

There are a number of behaviours that can threaten freedom of thought, including:

1. Censorship: Governments or other authorities may try to suppress certain ideas or beliefs by censoring information or punishing those who express certain viewpoints.
2. Intimidation: Threats, harassment, or violence against those who hold or express certain beliefs can deter people from thinking or speaking freely.
3. Propaganda: The use of misleading or biassed information to manipulate public opinion or shape people's beliefs can undermine freedom of thought.
4. Groupthink: Pressure to conform to the beliefs or opinions of a particular group can discourage independent thought and limit the diversity of ideas and perspectives.
5. Lack of access to information: If people do not have access to a wide range of viewpoints and sources of information, they may be limited in their ability to think freely and form their own opinions.

#socialfabric #ValuesFrameworks #SafetyProtocols

HumanCentric Digital Identity

This is intended to be a brief summary document providing some sense about the complexities involved in designing systems to support Human identity development and/or #HumanIdentity support systems, as is distinct to the use of the term #Identity or #DigitalIdentity in most (other) contexts.

This is not intended to be an exhaustive document on the topic.

The top Google definition of what 'identity', defines the concept as: *the fact of being who or what a person or thing is.* Yet this is not what most persons speaking about the concept from a perspective of their work or employer mean (note: SocialFactors). Most of the time what these people are talking about is some sort of identity related instrument or what Americans call 'Credentials'. In some circumstances, particularly within the field of #ICT #Cyber and #Internet what they're talking about is the way people 'log in', and in fields relating to finance they often mean the ability to verify their services are connected to a known entity for legal purposes such as anti-money laundering laws (#KYC AML) and similar; and whilst these constituencies relating to persons are very important, they're different to 'human identity' and have both different qualities and different sorts of needs.

The Human Centric AIApproach to better rationalising the concept of 'human identity' is a critically important foundational requirement for the entire ecosystem. As such, it is an instrumental part of the SafetyProtocols framework. Essentially, what the Human Centric AI environment does is provides a capacity for software agents to semantically and temporally support agent centric communications and personal stewardship of a person's own life, and therefore / thereby - their #Identity.

These concepts are somewhat linked with the Centricity considerations that are part of the informatics design principles. Therein, whilst 3rd parties will provide VerifiableClaims&Credentials they do not in and of themselves define who a human being is; they only provide artefacts related to that instrument and whatever it is says, only reflects the statements made on that verifiable document; it does not in and of itself, define a human being; nor does any private key related to the storage of that #Things. The greatest reason why others cannot properly define a person in a way that appropriately defines exactly who that person is; is that they'd need to know everything about that person, which is not possible for various scientific reasons.

So, there's a concept of #Observers which are in-turn dynamic with TemporalSemantics and what is in-effect a subset of PermissiveCommons.

In-effect, the #Human Centric AI environment is intended to provide support for #HumanIdentity in a particular way, that means the person is responsible for defining who it is they are, as a consequence of their actions - of what they do, what they don't do, etc.

This is then stored in a way that provides the owner of a #Human Centric AIto manage their identity and in-turn also, their Relationships(Social). These considerations are being assembled into useful tools that seek to have the effect of protecting FreedomOfThought and in-turn also address issues of significance, such as EndingDigitalSlavery. To achieve this, foundational requirements such as TheValuesProject works to create an #AI environment that is able to support complex technology related requirements.

In-turn, these systems are intended to support a methodology where Human Centric AIOwners, have the tools they need to be the primary steward of their own lives, and in-turn support also the means for those persons to both; protect themselves and their loved ones (including children & other dependants) from harms that the architecture of how information systems work today, enable and in-turn provide economic support for both enabling and processing Currencies gainfully by exploiters, at great cost.

Human Centric AI

Summary

Human Centric AI refers to the use of CognitiveAI in connection with Centricity considerations.

Human-Centric AI is a term used to describe artificial intelligence (AI) systems that are designed, in consideration of SocialFactors, to ensure that AI systems act as tools and not rulers. This is important for the preservation of #humanRights and an array of other considerations otherwise considered to be constituencies of the broader SafetyProtocols requirements and related WebScience Paradigms.

This type of AI is focused on creating technologies and systems that are both; able to support,

- Personalised AI Agents; tailored to the needs and preferences of humans, rather than simply optimising for efficiency or performance; and,
- Making sure that Centricity considerations apply to TemporalSemantics involving ArtificialMinds and indeed also more broadly; legal personalities

Human-centric AI systems may be designed to support and augment human cognition and decision-making, or to provide assistance and services to humans in a variety of contexts.

They may also be designed to be more transparent and explainable, so that humans can understand how the AI system is making decisions and take appropriate action based on those decisions.

Human-Centric AI is focused on creating AI systems that are tailored to the needs and goals of humans and that support and augment human cognition and decision-making, yet, the way in which this is achieved via Human Centric Principals, does not undermine our capacity to form a means to maintain support for Human Rights and Responsibilities; which is in-turn instrumental for ensuring support of Democracies, Rule of Law and other ValuesCredentials as is otherwise noted as being constituencies of the TheValuesProject.

Works are being progressed via community groups noted: http://www.humancentricai.org/

Values Credentials

Values Credentials are electronic instruments that can be used to support various types of relationships with other entities, agents, transactions and things. Values credentials are a type of VerifiableClaims&Credentials.

The term 'values' is intended to denote the concept of a person's (human being or guardian) 'human values' that need to be provided the apparatus to provide support for those values.

These tools are considered to be of instrumental importance for the development of Human Centric AIas 'peace infrastructure' both as a project, and as a toolset for the production of other projects.

The Values Credentials, provide support for how other agents are able to be managed. Rather than the concept of 'opt-in' or 'consent', the concept of 'values credentials' relates to 'human agency', and the ability and desirability for human beings as foundationally important active natural agents, to make wilful choices about how it is they want to organise their life; and in-turn also, how it is they're able to track and improve their own quality of being, and the growth of themselves as a person.

Users are able to use values credentials, to help them curate how they interact with other agents; and can even provide support for excluding themselves from other agents who do not share some particular common-value that is of great importance to that person / agent.

Importantly also, these systems are designed to support SocialFactors , Credentials&ContractsManager, AgentDirectory

Types of Values Credentials

Whilst some efforts have been made to attempt to categorise the values instruments, they are not provided in any particularly specified order; the order of importance is not necessarily reflected by the order in which they are listed below.

Once the WebizenTechStack and PCTOntologyModelling / PermissiveCommonsTech is adequately produced, these instruments will be encoded in RDF see: What is Linked Data if the concept of RDF (linked-data) is not understood...

The Charter of the Commonwealth.

International HumanRights values.

- Universal Declaration of Human Rights
- Universal Declaration on Cultural Diversity
- Universal Declaration on the Eradication of Hunger and Malnutrition
- Universal Declaration on the Human Genome and Human Rights
- Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind
- Declaration on the Right of Peoples to Peace
- Declaration on the Right to Development
- Declaration on the Rights of Disabled Persons
- Declaration on the Rights of Mentally Retarded Persons
- Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power
- Declaration of Commitment on HIV/AIDS

- Declaration on Race and Racial Prejudice
- Declaration on Social Progress and Development
- Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on Religion or Belief
- Declaration on the Elimination of Violence against Women
- Declaration on the Granting of Independence to Colonial Countries and Peoples
- Declaration on the Human Rights of Individuals who are not nationals of the country in which they live
- Declaration on the Protection of All Persons from Being Subjected to Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment
- Declaration on the Protection of all Persons from Enforced Disappearance
- Declaration on the Protection of Women and Children in Emergency and Armed Conflict
- Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms
- Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities
- United Nations Millennium Declaration
- Vienna Declaration and Programme of Action
- International Covenant on Economic, Social and Cultural Rights
- International Covenant on Civil and Political Rights
- International Convention against the Recruitment, Use, Financing and Training of Mercenaries
- International Convention for the Protection of All Persons from Enforced Disappearance
- International Convention on the Elimination of All Forms of Racial Discrimination
- International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families
- Slavery Convention
- Convention on the Rights of Persons with Disabilities
- Convention against Discrimination in Education
- Right to Organise and Collective Bargaining Convention, 1949 (No. 98)
- Indigenous and Tribal Peoples Convention, 1989 (No. 169)
- Convention on the Prevention and Punishment of the Crime of Genocide
- Convention on the Reduction of Statelessness
- Convention relating to the Status of Stateless Persons
- Convention on the Rights of the Child
- Convention relating to the Status of Refugees
- Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment
- Worst Forms of Child Labour Convention, 1999 (No. 182)

- Minimum Age Convention, 1973 (No. 138)
- Convention for the Suppression of the Traffic in Persons and of the Exploitation of the Prostitution of Others
- Convention on Consent to Marriage, Minimum Age for Marriage and Registration of Marriages
- Convention on the Elimination of All Forms of Discrimination against Women New York, 18 December 1979
- Convention on the Non-Applicability of Statutory Limitations to War Crimes and Crimes Against Humanity
- Discrimination (Employment and Occupation) Convention, 1958 (No. 111)
- Employment Policy Convention, 1964 (No. 122)
- Equal Remuneration Convention, 1951 (No. 100)
- Forced Labour Convention, 1930 (No. 29)
- Freedom of Association and Protection of the Right to Organise Convention, 1948 (No. 87)
- Supplementary Convention on the Abolition of Slavery, the Slave Trade, and Institutions and Practices Similar to Slavery
- Abolition of Forced Labour Convention, 1957 (No. 105)
- Code of Conduct for Law Enforcement Officials
- Guidelines for Action on Children in the Criminal Justice System
- Guidelines on the Role of Prosecutors
- Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law
- Basic Principles for the Treatment of Prisoners
- Basic Principles on the Independence of the Judiciary
- Basic Principles on the Role of Lawyers
- Basic Principles on the Use of Force and Firearms by Law Enforcement Officials
- Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment
- Geneva Convention relative to the Treatment of Prisoners of War
- Geneva Convention relative to the Protection of Civilian Persons in Time of War (2nd part)
- Rome Statute of the International Criminal Court
- General Assembly resolution 1803 (XVII) of 14 December 1962, "Permanent sovereignty over natural resources"
- United Nations Standard Minimum Rules for the Administration of Juvenile Justice (The Beijing Rules)
- Standard Rules on the Equalization of Opportunities for Persons with Disabilities
- United Nations Rules for the Protection of Juveniles Deprived of their Liberty
- United Nations Rules for the Treatment of Women Prisoners and Non-custodial Measures for Women Offenders (the Bangkok Rules)

- United Nations Standard Minimum Rules for Non-custodial Measures (The Tokyo Rules)
- United Nations Principles for Older Persons
- Principles on the Effective Investigation and Documentation of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment
- Principles for the protection of persons with mental illness and the improvement of mental health care
- Principles of international co-operation in the detection, arrest, extradition and punishment of persons guilty of war crimes and crimes against humanity
- Principles of Medical Ethics relevant to the Role of Health Personnel, particularly Physicians, in the Protection of Prisoners and Detainees against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment
- Principles on the Effective Prevention and Investigation of Extra-legal, Arbitrary and Summary Executions
- Principles relating to the Status of National Institutions (The Paris Principles)
- Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1)
- Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II)
- Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime
- Protocol amending the Slavery Convention signed at Geneva on 25 September 1926
- Protocol Instituting a Conciliation and Good Offices Commission to be responsible for seeking a settlement of any disputes which may arise between States Parties to the Convention against Discrimination in Education
- Protocol of 2014 to the Forced Labour Convention, 1930
- Protocol relating to the Status of Refugees
- Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime
- Optional Protocol to the International Covenant on Civil and Political Rights
- Second Optional Protocol to the International Covenant on Civil and Political Rights, aiming at the abolition of the death penalty
- Optional Protocol to the Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment
- Optional Protocol to the International Covenant on Economic, Social and Cultural Rights
- Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women
- Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography
- Optional Protocol to the Convention on the Rights of Persons with Disabilities

- Optional Protocol to the Convention on the Rights of the Child on a communications procedure
- Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict
- Safeguards guaranteeing protection of the rights of those facing the death penalty
- United Nations Guidelines for the Prevention of Juvenile Delinquency (The Riyadh Guidelines)
- Recommendation on Consent to Marriage, Minimum Age for Marriage and Registration of Marriages

We aim to produce material means to support the Sustainable Development Goals in a manner that is consistent with the principals otherwise outlined above.

Professional Charters

- International code of ethics for occupational health professionals
- DECLARATION OF GENEVA
- International Code of Ethics for Professional Accountants
- THE ICN CODE OF ETHICS FOR NURSES
- International Code of Ethics for Midwives
- International Bar Association: International Code of Ethics
- Information Technology and Moral Values
- ACM Code of Ethics
- ITPA
- AMA Code of Ethics
- Medical Board Code of Ethics
- Contributor Covenant
- Law Society of NSW
- Queensland Law Society
- Law Council of Australia
- APS Code of Conduct

Best efforts should be made to ensure works are FitForPurpose for efforts that seek to address Sustainable Development Goals in a manner that is consistent with the principals otherwise outlined above.

Citizenship Related Values

- Choice of Law (jurisdiction)
- Local Laws
    - Economic
    - Social
    - Criminal

Enforcement of Values

These values frameworks are some of many such forms of instruments that exist. The future TheValuesProject outcome is predominantly designed to provide the software required for people to more respectfully engage in contracts with others online directly between one another; and in-turn, they are also able to vary their agreements and make their own independent decisions about what to do in circumstances where values have been breached. To enable these systems, more work needs to be done during this development stage. As such, the ability to engender agency for persons in a manner that is considered FitForPurpose is not able to be better achieved until the technology that furnishes the means to do so, has been successfully accomplished. As such, the notes about the present-development stage is of instrumental importance until it is otherwise declared.

The present development stage

TemporalSemantics are kinda useful, so i'll make a note as of the time that i am now therefore writing this note. These notes will be updated overtime, and the information will be supplemented rather than replaced - save exceptional circumstances, etc.

3rd Feb 2023: notes

Pursuant to the notes made in the GuideForDevelopers and related WebizenTerms which is now therefore being developed primarily to support the WebizenDiscord channel; where there are conflicting values that are otherwise noted in one or more of the values related instruments noted above; a degree of BestEfforts to form a common-sense opinion / position, is overwhelmingly considered desirable. IF persons are unable to bind themselves to the general concepts that are embodied in these instruments, then do not get involved. Persons who are known to have wilfully acted in a manner that has sought to commit wrongs such as those described by the notes on SocialAttackVectors may be subject to banishmentExile without notice and without further regard, irrespective of employer or any other factor that may otherwise discriminatorily fail to adhere to the foundational principles described in the instruments above.

Once (webizen) systems are operational.

Arbitration of conflicting values.

The arbitration of matters involving alleged wrongs will be processed in accordance with the WebizenTerms stipulations; until such time as TheWebizenCharter and correlated WebizenAlliance infrastructure is able to be established; which in-turn requires a functional WebizenTechStack implementation, which is the purposeful activity that gives rise to the purpose of having written this and other notes here.

BestEfforts are to be undertaken at all times, however, all rights are reserved.

`#socialfabric #ValuesFrameworks #SafetyProtocols`

Protecting Children

Whilst a great deal of works were done up until the start of 2010; the greatest volume of work and related personal sacrifices that have been survived, was done as a consequence of my witnessing organised child-abuse being enabled by business systems in an area that is critical to the definition of the identity development of children. Whilst these adults, whom were mostly funded via the Government, made statements such to clearly state that the convention of the rights of the child played no role in their duties; and that, they were not able to provide any evidence or information that may be submitted to a court; irrespective of the tears and stories of why, as they spoke about being abused as a child, seeking me to feel sorry for them - rather than considering how it was that they were not able to be held accountable. PublicSectorWrongDoings is very serious. I wonder who is more dangerous; those who are professionally engaged in organised crime in the private sector, or those who do so with their colleagues in the private sector, but as public sector employees.

As I was writing Webizen3.0SetupUserExperience the need to make some design statements became clear. The Human Centric AIEnvironment and all related works are designed to protect the human rights of children and these requirements are non-negotiable. There is a lot that has been done, and a lot more that needs to be done; and in the interests of seeking to protect people - much of these works will need to be done via TrustFactory and related ecosystems (privately). As WebizenTechStack develops, SafetyProtocols will advance to protect children that will have consequences regardless of the employer or any adults involved. enough is enough - and there's alternatives for any persons who disagree and/or need to be expelled and/or clearly 'tagged' in the Human Centric AIEcosystem.

Related notes are per below;

There are many major use-cases relating to children specifically.

Whilst this is most certainly - front of mind - the design related statements to support the needs of children as being amongst the most important parts of the broader purpose; has not yet been documented formally; Noting also, it's actually quite difficult to do really well.

Whilst Webizen3.5 might find education industry customers - which would then in-turn bring about the works required to get these sorts of considerations sorted out far more quickly; previous experience of seeking to work with that segment in good faith - has not provided positive experiences at all. The term 'dodgy' comes to mind, in relation to my experience with some fairly significant 'stakeholders' in that space. Also, often they're somewhat lacking when it comes to considering the importance of the role of `family` as such, it may be important to ensure that support for `family` is provided before institutional curation of the HumanCentricDigitalIdentity of children; which, isn't necessarily going to stop them from advancing in these area as they are already; rather, it may act to protect children from the consequences of empowering dodgy and often unaccountable people whose practical associations with SafetyProtocols and SocialAttackVectors leave a lot to be desired; and hopefully, in future, (these) systems will act to clean-up those problems in remarkable ways - yet, there's going to be a volume of people who've been systemically engaged in behaviours that they may be ashamed of, but should fundamentally result in very serious penalties by law. As such, that issue about having to figure out how to address the people I simply noted as being dodgy; isn't considered to be simple, easy or feasible in the early-stages of this project.

It is fairly important to have a strongly fortified position before seeking to send child-abusers to a court of law where they may well face serious civil and criminal charges with consequence.

Resources associated to this field of work can be found in this part of the Peace Infrastrastructure Project Google Drive Library AiEthics/Children

Definition of 'Adult'; safety for persons who are 18-25?

In Australia, when a person reaches the age of 18 they are defined to be an adult who is lawfully responsible and entitled to do whatever they want (so long as it is legal); yet, i am unsure of whether a person who is 18 years old is fully (neurologically) developed; and, i also have concerns about the (sexual) exploitation of young people by much older people; which as far as i am aware, is a problem that is far more likely to be something that female may be impacted by (ie: prostitution linked with severe mental illness and no-safety protocols). Similarly yet different, it seems to me young male persons are more likely to get into trouble in relation to drugs (crime).

The social structures of defining the nature of requirements in relation to Human Development; is both important, and necessarily undertaken in a way that considers many complex issues; whilst seeking to leverage WebizenTechStack in ways that act to process various types of SocialAttackVectors and thereby also - empower appropriate prosecutions and any related compensatory measures that may be appropriately also applied usefully.

Relationships (Social)

The 'relationship management' safety protocol system is designed in consideration of human rights related principles, in addition to various social / temporal factors.

Often, the way 'connections' work online is that the way current relationships are categorised or classified is rudimentary and overly simplified. Then the way information is able to be managed if there is a change in that relationship status, is also over simplified - often, its friend, not-friend and/or block; and if someone is blocked, then anything that happened in the past, is all gone too!

So these over-simplified systems are susceptible to abuse; in all sorts of different ways, that are consequently very difficult to manage.

The principal concept relating to the management of social relationships, is built upon the use of the ValuesCredentials and the rules defined are generally (although there are some exceptions that are intended to be supported via other safety protocols) temporally applied; and if / when the rules change; and in-turn also, the circumstances change, then the patterns relating to the discovery, interaction and use of materials associated with the relationship also changes.

#socialfabric #ValuesFrameworks #SafetyProtocols

Fair Work Protocols

The Development of Fair Work Protocols, is an essential component to producing any solution that has any capacity whatsoever for EndingDigitalSlavery.

The Considerations relate to a problem that is fundamentally very old, and indeed also quite complex. In consideration, a lens of considering the past - in particular, the 8 hour movement and related historical contexts are thought useful when considering how a means to address these sorts of complex problems, might be addressed.

About the 8-Hour Movement

The 8-hour movement was a labour movement that sought to improve working conditions and protect the rights of workers by advocating for the reduction of the workday to 8 hours. The movement emerged in the late 19th century, at a time when many workers were subjected to long and gruelling workdays, often working 12 hours or more per day.

The 8-hour movement argued that reducing the workday to 8 hours would improve the health and well-being of workers, as well as increase productivity and efficiency. The movement used a variety of tactics to promote its goals, including strikes, boycotts, and lobbying efforts.

The 8-hour movement was successful in achieving many of its goals. In many countries, labour laws were enacted that set limits on the length of the workday and established the right to overtime pay for work beyond 8 hours per day. In the United States, the 8-hour movement played a key role in the passage of the Fair Labor Standards Act of 1938, which established the 40-hour workweek and established the right to overtime pay for work beyond 40 hours per week.

Overall, the 8-hour movement was a significant force in the fight for workers' rights and helped to improve the working conditions and well-being of millions of workers around the world.

Activities that are a form of work are those that are performed for the purpose of earning a living or producing goods or services. These activities may involve physical or mental labour and may be performed for an employer or as self-employment. Examples of work activities include:

1. Manufacturing goods
2. Providing services, such as consulting or healthcare
3. Teaching or lecturing
4. Performing research
5. Writing or creating content
6. Sales or marketing
7. Managing a business

Work activities are typically distinguished from recreation and sleep activities in that they are undertaken for the purpose of earning a living or producing goods or services, rather than for leisure or relaxation. However, it is important to note that what is considered work may vary depending on cultural and societal context, and some activities that are considered work in one context may be considered recreation in another.

The principles of the 8-hour movement, which sought to improve working conditions and protect the rights of workers in the industrial era, can be rejuvenated and applied to knowledge work in a number of ways. Some potential approaches could include:

1. Adjusting the focus: Rather than focusing solely on the number of hours worked, the principles of the 8-hour movement could be adapted to address issues specific to knowledge work, such as the need for flexibility, autonomy, and work-life balance.
2. Strengthening worker protections: Knowledge workers may not have the same level of legal protections as traditional workers, such as the right to unionise or the protection of labour laws. Policymakers and advocacy groups could work to strengthen protections for knowledge workers, such as by establishing new regulations or extending existing protections to cover this group.
3. Promoting fair compensation: Knowledge work can often be highly skilled and specialised, and knowledge workers may be entitled to fair compensation for their contributions. Advocacy groups and policymakers could work to promote fair compensation for knowledge work, such as by establishing guidelines or standards for fair pay.
4. Supporting education and training: The principles of the 8-hour movement could also be rejuvenated by supporting education and training programs that help knowledge workers to develop the skills and knowledge they need to succeed in their careers. This could include initiatives to promote lifelong learning and provide access to educational opportunities for knowledge workers.

Forming an applied Methodology for Knowledge Workers

There are many ways that the principles of the 8-hour movement could be rejuvenated and applied to knowledge work in order to support the rights and well-being of knowledge workers. By adjusting the focus to address the specific needs of knowledge workers, strengthening worker protections, promoting fair compensation, and supporting education and training, it is possible to create a more supportive and fair environment for knowledge work. This can help to ensure that knowledge workers are able to contribute their skills and expertise to society, while also being able to enjoy a high quality of life and work-life balance.

The nature of the concept of time spent engaged in work, recreation, and sleep activities for knowledge workers may differ from that of traditional workers in a number of ways. Some potential differences could include:

1. Flexibility: Knowledge work often requires a high level of flexibility, as knowledge workers may need to be able to adapt to changing demands and priorities. This may involve working outside of traditional business hours or working from different locations.
2. Autonomy: Knowledge workers may also have a higher level of autonomy, as they may be responsible for managing their own work schedules and priorities. This can allow for greater control over the balance between work, recreation, and sleep activities.
3. Boundaries: The boundaries between work, recreation, and sleep may be less clear for knowledge workers, as they may be required to be available and responsive to work-related demands outside of traditional business hours. This can make it more difficult to maintain a healthy balance between these activities.

The nature of the concept of time spent engaged in work, recreation, and sleep activities for knowledge workers may be more flexible and autonomous than for traditional workers, but it may also involve a greater challenge in maintaining a healthy balance between these activities.

Paying knowledge workers for the useful derivatives of their time spent doing work is important for a number of reasons:

1. Fair compensation: Knowledge work can often be highly skilled and specialised, and knowledge workers may be entitled to fair compensation for their contributions. Paying knowledge workers for the useful derivatives of their work can help to ensure that they are fairly compensated for their efforts and expertise.
2. Motivation and retention: Fair compensation can also be important for motivating and retaining knowledge workers. If knowledge workers feel that they are not being fairly compensated for their work, they may be less motivated to perform at their best or may be more likely to leave for other opportunities.
3. Intellectual property rights: Payment can also help to respect the intellectual property rights of knowledge workers. If knowledge workers are not compensated for their useful works, they may not have the financial resources to enforce their intellectual property rights or may be less likely to assert their rights in the face of potential exploitation.

Building an Equitable Future for Creators

Paying knowledge workers for the useful derivatives of their work is important for ensuring that they are fairly compensated, motivated, and able to assert their intellectual property rights. This can help to create a more supportive and fair environment for knowledge work, which can benefit both knowledge workers and society as a whole.

Income is often closely related to a person's ability to keep themselves safe, as having a steady and sufficient source of income can provide access to a range of resources and protections that can help to ensure safety and security.

For example, having a sufficient income can allow a person to afford basic necessities such as food, shelter, and medical care, which can help to ensure physical safety and well-being. Income can also provide access to financial resources that can be used to protect against financial risks, such as the ability to afford insurance or save for emergencies.

In addition, income can often be used to purchase goods and services that can help to ensure safety, such as security systems or emergency services. Having a sufficient income can also allow a person to afford legal representation or other forms of advocacy, which can be important for protecting their rights and interests.

income is often closely related to a person's ability to keep themselves safe, as it provides access to a range of resources and protections that can help to ensure safety and security.

Relationship to Web Science Tasks

There are a number of web science questions that could be investigated in order to support the development of fair work protocols for knowledge workers. Some potential areas of investigation could include:

1. Workflow and productivity: Web science research could explore how different workflows and technologies impact the productivity and well-being of knowledge workers. This could include studying the effects of remote work, flexible work schedules, and collaborative tools on worker outcomes.
2. Fair compensation: Web science research could also examine how to design fair compensation systems for knowledge workers, including exploring the use of algorithms and other tools to assess the value of different types of knowledge work.
3. Intellectual property rights: Web science research could also explore ways to protect the intellectual property rights of knowledge workers, including studying the effectiveness of different approaches to licensing and copyright.
4. Work-life balance: Web science research could examine how to support work-life balance for knowledge workers, including studying the impact of different work environments and policies on worker well-being.

There are many different web science questions that could be investigated in order to support the development of fair work protocols for knowledge workers. By studying these issues, web science can help to inform the design of policies and practices that support the rights and well-being of knowledge workers.

ESG Implications

ESG (Environmental, Social, and Governance) criteria can be related to the importance of developing fair work protocols for knowledge workers in a number of ways. For example:

1. Social criteria: Developing fair work protocols for knowledge workers could be considered a social issue, as it relates to the well-being and rights of workers. Ensuring that knowledge workers are treated fairly and are able to work in a supportive and healthy environment could be seen as a key element of a company's social responsibility.
2. Governance criteria: Fair work protocols can also be related to governance criteria, as they can help to ensure that a company is governed in a transparent and accountable manner. Developing and implementing fair work protocols can help to demonstrate a company's commitment to responsible and ethical business practices.

Overall, ESG criteria can be related to the importance of developing fair work protocols for knowledge workers in that they can help to ensure that companies are addressing key social and governance issues and are committed to responsible and ethical business practices. By considering ESG criteria in the development of fair work protocols, companies can help to ensure that they are contributing to a more sustainable and equitable society.

Ending Digital Slavery

see note about DigitalSlavery. When asking ChatAI about Ending digital Slavery, it provided the following feedback;

ChatAI Notes

There are a few different economic models that might be better suited to addressing the issue of unpaid or underpaid work, especially when it comes to knowledge workers. One approach could be to adopt a model that places a greater emphasis on workers' rights and the fair distribution of wealth. This could involve implementing policies that aim to reduce income inequality and provide a safety net for workers who are not being fairly compensated for their labour. Additionally, there could be a focus on providing training and education opportunities to help workers develop the skills they need to negotiate for better pay and working conditions. This could be coupled with stronger labour protections and enforcement mechanisms to ensure that workers are not exploited.

There are a number of behaviours that should be avoided in order to end digital slavery, including:

1. Exploitative working conditions: Employers should ensure that workers are not subjected to excessive or unreasonable workloads, and that they are provided with fair pay and benefits.
2. Forced labour: Employers should not use threats, intimidation, or coercion to force workers to perform labour against their will.
3. Lack of worker protections: Employers should provide workers with adequate protections, including safety equipment and training, to prevent accidents or injuries on the job.
4. Discrimination: Employers should not discriminate against workers on the basis of their race, religion, gender, nationality, or any other protected characteristic.
5. Harassment: Employers should have policies in place to prevent and address harassment, including sexual harassment, in the workplace.
6. Lack of transparency: Employers should be transparent about their labour practices and should allow workers to freely communicate their concerns and report any issues without fear of retribution.

The principles for ending digital slavery can also be applied to open-source projects done online cooperatively with others. For example, it is important to ensure that contributors to an open-source project are not subjected to exploitation or forced labour. This means that they should not be asked to work excessive hours or be paid unfairly for their contributions.

It is also important to ensure that contributors to an open-source project are treated fairly and with respect, and that there is no discrimination or harassment. This may involve having clear policies in place to address these issues and providing a safe and inclusive environment for all contributors.

Transparency is also important in open-source projects. Contributors should be aware of the terms and conditions under which they are working, and should be able to freely communicate their concerns and report any issues without fear of retribution.

Overall, it is important to recognize that the contributions of open-source volunteers are valuable and should be treated with respect and fairness. By following these principles, open-source projects can be more inclusive and sustainable in the long term.

Notes and Considerations

it is very difficult to simplify the notion of DigitalSlavery as is similarly the case in seeking to provide a simple summary of how it is these works act as a broad-ranging ecosystem with the express intent, of seeking to form apparatus that provides support for enabling lawful remedy in relation to these sorts of crimes and human rights abuses. As such, when considering the points made about ending digital slavery, note that the broader ecosystem, if effectively implemented; has an effect that is greater than any single part alone. The success of the project is effectively defined by whether and/or how it supports #RealityCheckTech, without unreasonably compromising other broader values. The Human Centric AI ecosystem produces an environment where technology, and by extension - Artificial intelligence, is curated as a set of tools for human kind to employ, as to be supported by those tools, and in-particular thereafter; be better equipped to be empowered to successfully engage in activities such as the broader PeaceInfrastructureProject - which is far less about ICT and far more about our biosphere and in-turn sociosphere; whereby, we need the tools to achieve more than is otherwise simply illustrated by the SDGs.

Knowledge Qualification Methods

The advent of AI, is far more significant than the implications of the time where calculators became easily accessible.

I've asked OpenAI / ChatGPT the following;

What are some practical courses of action that could assist educators in seeking to evaluate whether a student understands a topic or subject that they've been required to study, but may have used an AI program to produce a written report that is submitted - without necessarily understanding what it is the activity was intended to support the students ability to learn about and gain knowledge about, the topic. What sorts of activities could be undertaken to evaluate whether or not a student has gained knowledge about the topic, rather than more simply, having used an AI program to provide reports that may pass traditional tests without the student necessarily understanding or gaining knowledge of the topic, subject and/or related concepts.?

There are several practical courses of action that educators can take to evaluate whether a student understands a topic or subject that they've been required to study, even if they have used an AI program to produce a written report. Here are a few examples:

1. Oral or written questioning: One effective way to evaluate understanding is through oral or written questioning. The educator can ask the student to explain or summarise key concepts or ideas related to the topic, or to provide examples of how they apply the knowledge in a specific scenario.
2. Hands-on activities: Another way to evaluate understanding is through hands-on activities such as problem-solving exercises, lab experiments, or group projects. These activities allow the student to demonstrate their understanding of the topic in a practical setting.

3. In-class participation: Educators can observe and evaluate the student's level of understanding through in-class participation, such as group discussions, debates, or presentations. Through this, the educators can see the level of engagement and understanding of the student.
4. Self-reflection and feedback: Educators can ask the students to reflect on their learning process and provide feedback on the effectiveness of the learning methods they have used. Through this, the educators can evaluate if the student has gained knowledge about the topic or not.
5. Peer evaluation: Educators can also ask students to evaluate each other’s understanding of the topic, this can be done through a peer review or through small group discussions, where students can identify areas of misunderstanding and help one another to understand the topic better.
6. Use of Authentic Assessment: Educators can use tasks that are similar to what students may encounter in the real world, this allows students to apply their understanding of the topic in more meaningful and relevant context, thus evaluating the real understanding.

It's worth mentioning that this list is not exhaustive, and that each educator should choose the approach that they think is the best fit for the specific subject, students, and context. Additionally, a combination of several of these methods might yield more accurate results.

Another approach educators can take is to design assessments that are difficult for AI software to complete, for example, assessments that require students to integrate or apply multiple pieces of information, or that require creativity, critical thinking, or complex problem-solving skills. Such assessments are more likely to be difficult for AI software to complete as they are not based on simple pattern recognition, but on sophisticated abilities that are characteristic of human intelligence.

Additionally, incorporating more open-ended questions that require students to provide explanations or to justify their reasoning can also be an effective way to evaluate whether students have a deep understanding of the topic, rather than just recognizing patterns in the text.

In addition to these approaches, educators can also use plagiarism detection software to identify instances where students have used AI to produce written reports without understanding the topic. However, it is important to note that plagiarism detection software is not a foolproof method, as it can only detect text that has been copied and pasted from other sources, not text that has been generated by AI.

Finally, Educators should also be aware of their own role in fostering the critical thinking and understanding of the students, by providing clear learning objectives, providing appropriate resources and providing opportunities for feedback and continuous improvement.

No Lock-ins

There are a variety of unwanted behaviours, that are often commercially motivated, that engender some form of lock-in that is contrary to the interests of TheValuesProject and in-turn also, TheWebizenCharter, WebizenAlliance and other related considerations.

In-order to support a means to maintain the hygiene of these environments and the underlying moral integrity of the broader objective, DataPortability is being designed as one of the SafetyProtocols.

Others include;

Golden Handcuffs

I've been using the term 'golden handcuffs' for some time, and only recently reviewed the definition provided for the Concept Golden Handcuffs, finding that the meaning was in many ways different to what it was I was trying to describe. Therein; my thoughts on the golden handcuffs issue, was basically about entrapment; or the means to create 'lock-ins' that bind a person to a particular commercial provider or situation that is harmful to them, because circumstances are engendered to ensure the cost of leaving (or 'doing the right thing') is made to be more costly than simply doing what is expected of another entity, subserviently. Online, this often links with practices that seek rents from users by creating a situation where they're unable to exist or have meaningful support of their own human rights or have negative impacts if they decide to stop depending upon the 'things' you specifically provide them.

Data Portability

Data Portability is an essential requirement for various reasons. Whilst the Human Centric AI environment is being designed to support the ability for people to own their own 'Webizen', there are still components that need to be operated on the network, most likely via some sort of infrastructure solution that's being provided via ICT Operating in a Data Centre somewhere. This "Head End" or gateway counterpart; is intended to be made available in a way that means Human Centric AIOwners can set one up themselves. Nonetheless, the Human Centric AI protocols feature an array of ValuesCredentials that may in-turn lead to a user wanting to migrate their entire environment to some alternative system.

So, whilst the qualities of how these systems work is very different to the way Web 2.0 apps work; there are still a series of requirements, both in seeking to obtain information from legacy systems, and also to support the needs of a user should they want to migrate.

The Data Portability Project whose Current Contributors include Apple, Facebook, Google, Microsoft, SmugMug and Twitter is an example, and the GitHub Repo for it is: google/data-transfer-project

Most other platforms have some sort of API and/or Export function, and there is a means to write software that can provide either or both; the means to transfer information to a Human Centric AI platform in future, or alternatively interact with the external platform via an API.

Solid & Similar

Solid is the name of a critical foundational body of work that relates to the historical Human Centric AIrelated body of works both by W3C related Communities, involving also myself (Web Civics / Trust Factory; knowledge banking, etc) body of works.

These works also involved various other W3C Community efforts (projects); the intended purpose was to end-up with the tools required to create an ecosystem that was supported by open-standards (w3c, ietf, etc).

Solid is now led by Inrupt which was co-founded by the Inventor of the World-Wide Web, Sir Tim Berners-Lee, He is presently working towards a W3C Solid Working Group

I celebrate the significance of the attention TimBL has prioritised towards these efforts. It was certainly the case earlier, that progress was impossible and indeed very dangerous, as such his commitment towards progressing this work; has led to progress that wouldn't have occurred otherwise.

Yet, For reasons I would prefer not to discuss fully publically (seems inappropriate), the Human Centric AIProject is seemingly quite different to what it is that they've been working to create.

Nonetheless; part of the objectives, as to support the safety protocols requirements; should be to seek to ensure owners of Human Centric AIsystems can migrate to something else that can provide the highest level of compatibility or similar features, as is possible. This is both a moral requirement as well as it being a practical requirement.

The Human Centric AIEcosystems has an array of Values Frameworks, which are sought to be enforceable. This may mean that a person who is shown to have acted in a way that invokes the need to act as to protect the rights of others in a way that is considered extremely serious; and ideally also, as should in-turn be made able to be considered by a court of law; then, the consequences may be that the TemporalSemantics are considered negative to an extent whereby the Human Centric AI owner wants to migrate away, to a system that may in-turn support different Values (ie: an environment that does not support ValuesCredentials).

As such, Whilst there are an array of very difficult considerations that need to be worked through as a WebScience problem, the underlying belief is that the closest technical solution; is likely to be related to the Solid Specifications and in-turn solid protocol which needs to be supported for interoperability purposes anyway.

From an Artificial Intelligence perspective, a means for people to migrate needs to be considered. the options to achieve these sorts of outcomes, have not been evaluated yet.

It is expected that there will be an array of qualities that the Human Centric AI & Web Civics Ecosystems will offer that are not otherwise available. Whilst it is likely that the creation of a solution will invoke a market of competitors creating similar works; it is still likely to be the case that there will be significant differences.

3rd Party Rights

The means to ensure that a person, regardless of their circumstances, are able to migrate; should not disaffect or cause injury to others. This needs to be considered also, as there are various consequences that are not purely about 'data portability', but rather social informatics more broadly.

Enforceability of Rules

Whilst very best efforts are being made to seek to ensure that the environment addresses SocialAttackVectors and other threats that may otherwise cause harm to persons in a manner that is unfair; part of what is required to achieve these sorts of outcomes, is, at the end of the day - the ability for a TheWebizenCharter, WebizenAlliance member to boot a person off their system and cease to provide any support or assistance for that entity.

Whilst this does not mean that a provider has any right to decide any lawful punishment that may apply to the subject of any such form of action; and whilst any judgement made by an appropriate legal tribunal and/or court of law (or indeed also via legislature); there is also an array of obligations that are built into the Human Centric AI ecosystem which require stewards (alliance charter / Human Centric AI alliance members / values-credentials related agents) to process and consequently address. If the consequences of those circumstances result in an outcome that means the data-subject is excommunicated; then, they still need to be provided the means to have somewhere else to go.

There are also an array of Ontological Notations that are necessarily produced, as to provide an VerifiableClaims&Credentials that will be rendered against TemporalSemantics and ensure any disaffected parties may take any further disputes to a court of law for review and/or lawful determinations in relation to the circumstances, etc.

Objectively, this is not the sort of event that is sought to occur; however, there are circumstances where the nature of a person's actions is of a kind, that requires action and most often these circumstances would also invoke a situation where reporting a matter to an appropriate law enforcement body should be part of the procedural processes employed by WebizenAlliance members. However, it is not always the case that situations of a serious nature end-up being investigated or appropriately investigated; in which case, the consequence of on-going harms that may otherwise occur is not considered to be supportive of any factors relating to the CommercialModels including but not limited to ESG considerations, and it is important that there is a right to act; and to seek to form SocialFactors related considerations about how to address complex issues in a proportionate and responsible manner.. These sorts of works are complex and will require time and expertise of various persons, which is in-turn only reasonably able to occur after the Webizen 3.0 solutions are operationally in-place. An interim solution will be required before that occurs.

Data Formats

Most of the data-systems are designed using Semantic Web technologies; or in other words, it's put together using an ecosystem of open-standards in a specified manner, to create something new. Nonetheless, the underlying data (semantic web structures, etc.) can, somewhat easily, be exported in formats that can be usefully employed by other 'apps'; but, the ecosystem's solution characteristics aren't simply about the data-format of the data only.

To Some-Degree, attempting to migrate away from the Human Centric AI environment, may become as difficult as seeking to migrate away from the use of InternetStrategy where there is no alternative that performs a similar sort of function (yet - noting the future for Blockchains, is unknown).

Banishment & Exile.

Below are some notes produced via ChatGPT, however, as an introduction to the concept generally; the WebScience study and objective challenge is to define; answers to questions that include but are not limited to the following,

- under what terms and circumstances should a person be rightfully exiled from the WebizenAllianceHostProviders platform and/or other WebizenAlliance tools and services.
- What are the conditions that must be met, what are the responsibilities and duties connected with any such act; how are the decisions to apply such forms of penalties formed, whom by, what evidence is required and what requirements exist in relation to the communication of that evidence; to whom, for what purpose, etc.
- Given the systems are premised upon the idea that the Human Centric AI owner - owns their 'webizen' (hardware/software) - what does the penalty incur; and what is left for them.
- Is there a duty and/or responsibility for any WebizenAlliance member to be required to communicate what information about the event and under what circumstances, terms and to whom.

IF a person who is instrumental to the development of this work, has been previously seriously injured by another legal entity or definable members of a group; and perhaps these matters are unresolved. Is a right to deny access allowed? If so, under what circumstances? how might wrongful behaviour be reasonably addressed as to ensure persons are not subject to continued harm consequentially.

These are the sorts of questions that require a moral approach far more than simply a technical approach. This in-turn links with the SocialContractGamification issues, alongside other SocialAttackVectors and related SafetyProtocols.

COURT OF LAW: PRIORITISED

These considerations are not intended in any way to usurp the dutiful social doctrines that define the appropriate venue for resolving conflict in a manner that is consistent with all ValuesCredentials to be appropriately administered by way of a court of law or appropriate venue of lawful arbitration. Indeed a major objective of Human Centric AIis to empower the ability for vulnerable persons to seek lawful remedy via a court of law particularly in the most desperate of circumstances. Nonetheless, this is often not reasonably available to persons who have been subjected to wrong-doing.

ChatGPT Notes: About Banishment & Exile

In mediaeval times, being expelled from a community and banned from returning was a serious punishment, often referred to as "banishment" or "exile." Banishment was a common punishment for a variety of crimes and offences, including theft, murder, and other serious crimes, as well as political and religious dissent.

The exact terms and conditions of banishment varied depending on the time period and the jurisdiction, but in many cases, the person who was banished would be forced to leave the community and was not allowed to return without permission. They were often stripped of their property, rights, and privileges, and they could be subject to further penalties, such as imprisonment or even death, if they were caught returning.

In some cases, banishment was imposed for a fixed period of time, after which the person could return to the community. In other cases, banishment was a permanent punishment, and the person was permanently banned from returning.

The use of banishment as a form of punishment declined in the modern era, as societies developed more sophisticated and humane forms of punishment. Today, banishment is generally considered to be a form of cruel and unusual punishment, and it is not used as a form of punishment in most countries. Instead, individuals who have committed crimes are generally punished through imprisonment, fines, or other forms of punishment that are deemed to be more appropriate and humane.

In the case of the Hashshashin and the samurai, banishment and exile were used as penalties for various offences and crimes. The causes, practices, and terms of these penalties varied depending on the specific group and the historical context.

For the Hashshashin, banishment and exile were used as a form of punishment for members who broke the group's strict code of conduct, as well as for political and military reasons. The specific terms and conditions of banishment and exile would have varied depending on the situation and the circumstances.

For the samurai, banishment and exile were used as a form of punishment for offences such as insubordination, dishonourable conduct, and other crimes. The specific terms and conditions of banishment and exile would have varied depending on the individual case, the samurai's status and rank, and the political and military context of the time.

In both cases, banishment and exile were considered serious penalties that carried a significant social and cultural stigma. The individuals who were subjected to banishment and exile were often seen as having brought shame upon themselves and their families, and they faced significant difficulties in reintegrating into society.

Overall, while the causes, practices, and terms of banishment and exile varied depending on the specific group and the historical context, these penalties were generally used to enforce codes of conduct and to maintain social order and stability. The penalties of banishment and exile were also considered to be a form of social control, and were used to maintain the power and authority of the ruling class.

Guardianship Semantics

Introduction

There are various types of situations where 3rd parties have some sort of legal duty in relation to others. Common examples include children, elderly persons and those with severe disabilities, that act to impair their ability to be independently capable of managing their own lives and/or rights and responsibilities.

When seeking to form an information systems methodology to support personal human agency and fundamental support for the human rights of all persons; this area of decision making appears to be a particularly difficult area to define what the most appropriate rules and related requirements should be. It is not uncommon for persons who are subject to guardianship relations / duties, as are enacted in some way that has the effect of others being responsible for that person; to be used in a manner that does not serve their best interests. Equally, the interpretation of what may be in their best interests vs. what it is that any such person subject to any such form of legal framework wants, may be quite different.

In some cases; there is no good legal standing that exists to more easily support information management related assertions via WebizenAlliance related systems and authorities; which in-turn, likely invokes a requirement to form appropriate SafetyProtocols that provide a series of policies and responsibilities about how various types of situations are judged to be best handled; and in-turn also, what the repercussive implications may be in circumstances where these sorts of rules are subject to some form of improper SocialAttackVectors related event.

This document will be expanded upon to further define some high-level considerations about how it is that these sorts of requirements will be addressed on a BestEfforts basis

Guardianship Relations

The work to figure out the AccountCreation and GuardianshipSemantics to provide SupportForHumanAgency for persons who require assistance from others, has been something that I've sought to find solutions to address for a very long time. Indeed the means to address these requirements is essential for HumanCentricDigitalIdentity and HumanCentricAI. Despite best efforts in seeking input from the government and others involved in digital identity and e-safety, any useful feedback has been difficult to discover. It just hasn't been provided, perhaps, because it either hasn't been considered or that the way in which it is sought to be addressed is a subject related to shame and those involved just don't want to talk about it. Irrespective of why, some progress was made by entering the query and related considerations to ChatGPT, which provided information below.

Description provided to ChatGPT:

I am working on software that supports entity logic.

In this design logic;

The term Entity Centric refers to legal entities, whether they be individual natural persons or legal persons (incorporated entities, government entities, etc.).

The terms Agent Centric and Agent refers to things that do stuff. A well known sub-class is Person, representing people. Other kinds of agents include Organizations, Groups, software and other 'things'. and,

The term Human Centric refers to the orientation of information management systems that centre upon the rights, responsibilities and moral ownership of electronic records pertaining to a human being.

Some Human Beings are not able to make legal decisions or hold legal responsibility on their own behalf. This may be due to disability, psychiatric illness, ageing related conditions, emergency medical situations as well as consideration for the needs of children. This may be considered to relate to persons who have some sort of guardianship requirements to support the person's human rights.

If each Adult Human being is able to own, store and operate their own data / information and manage their own authentication and permissions systems, but that this cannot be achieved for persons who require some sort of guardianship support; how could systems be designed to support the safety and human dignity / human rights of persons who require guardianship related shared permissions structures and how could those permission structures be defined to support the persons human rights / human dignity?

Chat AI:

In terms of technical solutions, systems can be designed to support flexible permission structures that can be tailored to the specific needs of each individual. For example, the system could allow for different levels of access and control depending on the individual's needs and abilities. For example, individuals who require more support may have more limited access to their data, while those who are able to make decisions on their own may have more autonomy.

In terms of policy-based solutions, systems can be designed to incorporate principles such as transparency, accountability, and privacy by design. These principles can help ensure that the system is designed with the protection of the individual's rights and dignity in mind, and that any decisions or actions taken on their behalf are fully justified and transparent.

In addition, having clear protocols for guardianship and determining guardianship, and clear transparent communication channels for guardianship decision making would be essential. This can be achieved by having legal frameworks that clearly outline the responsibilities and rights of all parties involved, as well as regular reviews to ensure that the individual's needs are being met and that the guardianship is still needed.

Ultimately, it is important to involve individuals who require guardianship, their guardians and other stakeholders in the design process to ensure that the system is tailored to their specific needs and that it meets their safety, security and human rights standards.

Q: if a person who requires guardianship is defined as a dependant; who still retains human rights, but is dependant upon one or more others to be supported to maintain a beneficial relationship with those rights; What technical designs could provide the dependent their own digital human agency, perhaps through the ownership of a database that contains their information; but is supported by others who also have access? how might the information be categorised to appropriately provide support, as well as maintaining the defendant's right to privacy and freedom of thought?

ChatGPT: *One approach to providing a dependent with their own digital human agency, while also supporting them with access to their information, could be to use a decentralised database system. This type of system would allow the dependent to have control over their own data, while also allowing designated individuals, such as guardians, to have access to the data as needed.*

The information in the database could be organised in such a way that it supports the dependent's needs and rights, while also protecting their privacy. For example, sensitive personal information could be kept private and only shared with designated individuals on a need-to-know basis. Information that is needed to support the dependent's daily needs could be more easily accessible by their guardians.

One way to organise the information to support the dependent is to use a hierarchical structure where personal data is separated into different levels of privacy and accessibility. For example, the dependent could have full control over the highest level of data, which includes information such as their medical history, contact information, and personal preferences. The lower level of data is shared with the designated guardians or support people and it can contain information such as appointments, social and other interactions that the dependent would have.

Another design solution could be to use a permission-based system, where the dependent and their guardians can assign different levels of access to the data for different individuals or groups. For example, the dependent may allow their primary guardian to have full access to all of their data, while other family members or caregivers may have more limited access. Additionally, consider setting up expiration dates for access, so that the data is not indefinitely accessible.

To maintain the dependent's right to privacy and freedom of thought, it is also important to have clear policies and procedures in place for handling data, as well as regular audits to ensure that the system is in compliance with regulations, standards and to assure dependant's information is being handled appropriately. Additionally, involving the dependant in the decision making process and choices of the systems, protocols and policies that would be employed to support their human agency can help ensure that their needs and rights are being met.

Another important aspect of maintaining the dependent's right to privacy and freedom of thought is to provide them with the necessary tools and resources to understand and manage their own data. This could include providing training and education on how to use the database and permission system, as well as giving them access to clear and easy-to-understand information about their rights and the policies and procedures that apply to their data.

Additionally, involving the dependent in the decision-making process when it comes to the use of their data, can be essential. For example, they can have a voice in which of the data they allow to be shared with which parties, and under what conditions.

Finally, it is important to have robust security measures in place to protect the dependent's data from unauthorised access or misuse. This can include using encryption, secure authentication methods, and regular backups to protect the data from loss or damage.

In summary, providing a dependent with their own digital human agency can be achieved through the use of decentralised databases and permission-based systems that allow the dependent to have control over their own data, while also allowing designated individuals to have access as needed. The system should be designed to support the dependent's needs and rights, while also protecting their privacy, including through the use of hierarchical data structure, expiration date of access, and involving the dependent in the decision making process of sharing and managing the data. To maintain dependant's rights, security measures must be in place, as well as clear policies and procedures for handling the data, regular audits and involving dependant in the decision making process.

Q: What sorts of policy based mechanisms would be required and/or beneficial to support the human rights of the dependent?

ChatGPT:

There are a variety of policy-based mechanisms that can be implemented to support the human rights of a dependent. Some of these include:

1. *Clear legal frameworks: Establishing clear legal frameworks that outline the rights and responsibilities of all parties involved in supporting the dependent, including their guardians, caregivers, and family members. These frameworks should also provide guidelines for decision making and dispute resolution.*
2. *Human rights-based approach: Ensuring that the approach taken to support the dependent is based on the principles of human rights, including the right to autonomy, privacy, and dignity. This should include regular reviews of the dependent's needs and the effectiveness of the support being provided, to ensure that their rights are being respected.*
3. *Transparency and accountability: Implementing systems and procedures that promote transparency and accountability in the handling of the dependent's data and in the decision-making process around their care. This can include regular reporting, regular audits, and mechanisms for addressing grievances.*
4. *Privacy and security: Developing and implementing policies and procedures that protect the dependent's privacy and personal information, including strict protocols for data handling, regular security reviews, and the use of encryption, authentication and access control mechanisms.*
5. *Participation and informed consent: Involving the dependent in the decision-making process, providing them with the information necessary to understand the choices being made, and ensuring that they are able to provide informed consent.*
6. *Independent oversight: Having independent oversight and regular review mechanisms to ensure that the dependent's rights are being respected and protected, and to identify and address any concerns or issues that may arise.*
7. *Monitoring: Establishing regular monitoring, reporting and review mechanisms to ensure compliance with the above mentioned policy based mechanisms and identify and address any issues.*

It is important to note that, depending on the specific context and needs of the dependent, additional policy mechanisms may be necessary to ensure their human rights are protected.

Q: If a dependant is unable to independently own or lawfully protect (ie: via courts of law) their own rights relating the ownership, storage and use of their own personal and private information; how might a legal structure be devised to support their needs, with the support of others?

ChatGPT:

If a dependent is unable to independently own or lawfully protect their own rights relating to the ownership, storage, and use of their personal and private information, a legal structure could be devised to support their needs with the support of others.

One approach could be to establish a legal guardianship or conservatorship system. This would involve a legal process where a designated guardian or conservator is appointed by a court to make decisions on the dependent's behalf regarding their personal and private information. The guardian or conservator would be responsible for managing the dependent's data and ensuring that their rights and interests are protected.

Another approach could be to establish a legal trust, where the dependent's data would be held in trust by a designated trustee. The trustee would be responsible for managing and protecting the dependent's data, in accordance with the terms of the trust and any court orders. This legal trust can be tailored to the specific needs of the dependant and the level of autonomy they wish to retain.

The legal structure that is chosen would need to be in compliance with the local jurisdiction laws, while also taking into account the needs and autonomy of the dependent person. Additionally, it would need to be reviewed and updated on a regular basis.

In both cases, the legal structure would need to provide for oversight and accountability to ensure that the dependent's rights and interests are protected, and to address any issues or concerns that may arise. This could be through regular reporting, regular reviews, or mechanisms for dispute resolution, as appropriate.

It is also important to consider involving a range of stakeholders in the design and implementation of such legal structures, such as the dependant, their guardians, family members and other support people. This will help ensure that the legal structure meets the specific needs of the dependent, respects their autonomy and rights, and is tailored to the dependent's individual needs and circumstances.

Another approach to support the needs of dependants with the support of others could be by creating a power of attorney (POA). A power of attorney is a legal document that gives someone else the authority to make decisions on behalf of the person who has granted the POA. This could be a general POA which gives someone the authority to make all types of decisions, or a specific POA which gives someone the authority to make specific types of decisions related to personal and private information. In this case, the person granting the POA (the principal) would have the right to choose who their attorney-in-fact (the person they have chosen to act on their behalf) will be, and what kind of power they will have. The attorney-in-fact should act in the best interest of the principal, and in this case of the dependent, the attorney-in-fact would manage the dependent's personal and private information according to the terms of the POA and the best interest of the dependent.

Another potential legal solution that might support dependents and their rights over their personal and private information, could be the creation of a legal representative. This could be a person, or an organisation that is legally designated to represent the dependent in the management and protection of their personal and private information. This legal representative would be responsible for making decisions related to the dependent's information, such as sharing it with others or managing the privacy settings, and would act in the best interest of the dependent, while also complying with legal requirements.

It is also important to mention that, any solution that is chosen, it should not limit or restrict the dependent's rights more than is necessary to protect their best interests and they should be included in the decision making process and have the right to revoke the legal structure if they choose to do so.

In summary, there are a number of legal structures that can be devised to support the needs of dependents with the support of others, such as legal guardianship or conservatorship, legal trust, power of attorney, and legal representation. The specific legal structure chosen will depend on the jurisdiction and the specific needs and circumstances of the dependent. It is important to note that, regardless of the legal structure chosen, it should prioritise the dependent's autonomy and rights while also ensuring they are protected and their best interest is taken into account.

Q: How could a solution that attends to the considerations provided earlier; be devised using contract law between private individuals, that may in-turn expire as a consequence of some sort of condition having been met?

ChatGPT:

It is possible to devise a solution using contract law between private individuals that attends to the considerations provided earlier and that may expire as a consequence of some sort of condition having been met. One example of such a contract could be a personal data management contract.

This type of contract would outline the terms and conditions of how the dependent's personal and private information will be managed and protected. The contract would be between the dependent (or the person legally responsible for them) and the person or organisation designated to manage their data, such as a guardian, attorney-in-fact, or legal representative. The contract would include information such as the scope of the data that is being managed, the rights and responsibilities of each party, and the conditions under which the contract may be terminated or modified.

The contract could include an expiration clause, which would specify a certain condition or set of conditions that, when met, would result in the contract coming to an end. For example, the contract could expire when the dependent reaches a certain age or when their condition improves to a point where they are able to manage their data independently.

In addition, the contract should include provisions for regular reviews of the terms and conditions of the contract to ensure that it is still meeting the needs of the dependent and that their rights are being protected. It should also include provisions for dispute resolution, in case of any disagreement about the contract's terms or the management of the data.

It is important to note that any contract involving personal data should comply with relevant data protection laws, privacy laws and human rights laws, and that the dependent should be involved in the contract creation, review and termination process.

In summary, a solution that attends to the considerations provided earlier could be devised using contract law between private individuals. This contract, such as a personal data management contract, would outline the terms and conditions of how the dependent's personal and private information will be managed and protected and includes an expiration clause that specifies a certain condition or set of conditions that, when met, would result in the contract coming to an end. It should also include provisions for regular reviews and dispute resolution and comply with relevant data protection laws, privacy laws and human rights laws.

Another important aspect of this type of contract would be its enforceability. It's important to make sure that the contract is legally binding and that the rights and obligations of the parties are clearly defined and enforceable in court if needed. This can be done by including specific language in the contract that makes it clear that it is intended to be legally binding and that the parties have read and understood the terms of the contract before signing.

Additionally, it would be beneficial to consider involving legal professionals in the drafting and review of the contract, to ensure that it meets the legal requirements and that its terms are fair and reasonable to all parties involved.

It's also worth noting that, in some cases the contract could be used in parallel with or as part of a legal framework that is established by the government such as a guardianship or conservatorship structure, or a legal trust. In this case, the contract would need to be aligned with and comply with the legal framework that is in place.

In summary, a solution that attends to the considerations provided earlier could be devised using contract law between private individuals, that may in-turn expire as a consequence of some sort of condition having been met. This type of contract would provide clear and enforceable terms and conditions for the management and protection of the dependent's personal and private information, and would include an expiration clause that specifies a certain condition or set of conditions that, when met, would result in the contract coming to an end. It should be legally binding and comply with relevant data protection laws, privacy laws and human rights laws. It's recommended to involve legal professionals in the drafting and review of the contract, to ensure that it meets the legal requirements and its terms are fair and reasonable for all parties involved.

Q: make a list of the types of circumstances relating to a human being for whom these sorts of requirements are needed to support.

1. *Children or young people who are not yet legally able to make decisions about their own personal and private information*
2. *Individuals with cognitive or developmental disabilities that impede their ability to make decisions about their own personal and private information*
3. *Elderly individuals who are experiencing cognitive decline or have diminished capacity to make decisions about their own personal and private information*
4. *Individuals with mental illness that affects their ability to make decisions about their own personal and private information*
5. *Individuals who are in emergency medical situations and unable to make decisions about their own personal and private information*

6. *Individuals who are incapacitated as a result of a physical or neurological injury or illness*
7. *Individuals who have a temporary or permanent loss of consciousness or brain function*
8. *Individuals who are in a state of extreme distress and unable to make decisions about their own personal and private information*
9. *Individuals who are under the care of a court-appointed guardian or conservator*
10. *Individuals who are in a long-term care facility or receiving in-home care.*
11. *Individuals who have suffered a traumatic event or have been victims of abuse, which may affect their ability to make decisions about their own personal and private information.*
12. *Individuals with addiction or substance abuse problems that impede their ability to make decisions about their own personal and private information.*
13. *Individuals who are in prison or detention centres, and may be limited in their ability to make decisions about their own personal and private information.*
14. *Individuals with a history of homelessness, or who are currently experiencing homelessness, and may have limited access to information management and technology.*
15. *Individuals who are living in remote or rural areas, and may have limited access to services and support that would help them manage their personal and private information.*

It's important to note that this list is not exhaustive and there may be other types of circumstances where support to manage personal and private information is needed, it's important to evaluate each situation and the needs of the person on a case by case basis.

It's important to keep in mind that individuals may experience temporary or permanent changes in their abilities and require different levels of support to manage their personal and private information. The key is to work with the individual and assess their specific needs to provide the appropriate level of support and to make sure that their human rights and autonomy are respected.

Q: Please define an ontology using RDF, RDFS, OWL SKOS, SOIC and SHACL that illustrates an example of how this might work.

An ontology using RDF, RDFS, OWL, SKOS, SHACL and SOIC to illustrate an example of how this might work would be a complex task, as it would involve several steps, such as identifying the classes, properties, and relationships in the domain, defining the concepts and their hierarchies, and specifying the constraints and rules that govern the data.

However, I can provide an overview of how such an ontology might be structured, and some examples of the types of classes, properties, and relationships that would be used to represent the domain.

- *RDF (Resource Description Framework) would be used to define the basic structure of the ontology, providing a way to represent resources and the relationships between them.*
- *RDFS (RDF Schema) would be used to define classes and properties, and to provide a way to specify the hierarchical relationships between classes and properties.*
- *OWL (Web Ontology Language) would be used to provide more advanced modelling features, such as expressing cardinality and property restrictions, and defining classes and properties as equivalent or disjoint.*

- *SKOS (Simple Knowledge Organization System) would be used to express concepts and their relationships, and to provide a way to organise and browse the concepts in the ontology.*
- *SHACL (Shapes Constraint Language) would be used to specify constraints and rules that govern the data, such as data types, cardinality, and allowed values.*
- *SOIC (Supporting Open Identity & Control) would be used to express information related to the human identity, their rights, and access management.*

As an example, the ontology might include classes such as "Dependent", "Guardian" and "Data Manager", where "Dependent" would be a subclass of "Person" and "Guardian" and "Data Manager" would be subclasses of "Agent". The classes would be related through properties such as "hasGuardian" and "hasDataManager" where the properties would be defined as object properties linking "Dependent" with "Guardian" and "Data Manager" respectively. The ontology would also include classes such as "Personal Information" and "Privacy Rights" which would be related through properties such as "hasPersonalInformation" and "hasPrivacyRights" where the properties would be defined as object properties linking "Dependent" with "Personal Information" and "Privacy Rights" respectively. The ontology might also include properties such as "accessLevel" and "permission" which would be defined as data properties linking "Dependent" with "Personal Information" and "Privacy Rights" respectively, to indicate the level of access and permission granted to the different parties involved.

The ontology would also include a class "Data Management Contract" which would be related to "Dependent", "Guardian", "Data Manager" and "Personal Information" through properties such as "hasContract", "hasDependent", "hasGuardian", "hasDataManager" and "hasPersonalInformation" to indicate the parties involved and the terms and conditions of the contract.

In addition, the ontology could also include classes such as "Data Protection Law", "Privacy Law" and "Human Rights Law" that would be related through properties such as "compliesWith" linking "Data Management Contract" with "Data Protection Law", "Privacy Law" and "Human Rights Law" respectively to indicate the laws that the contract must comply with.

It's important to note that this is a high level example and the details of the ontology would have to be fleshed out further, with a more detailed understanding of the domain and specific requirements. Also, the use of different vocabularies and ontologies, it is important to ensure that the ontology is consistent and coherent and that the different vocabularies and ontologies are used in a way that is consistent with their intended purpose. In addition, it is important to use established vocabularies and ontologies when they are available, to make sure that the ontology is compatible with other ontologies and can be integrated with other systems.

Furthermore, one important aspect of the ontology is to make it flexible, to allow for future changes and extensions. It should be easy to update, to add new classes, properties and relationships, and to change the existing definitions as new information is acquired.

In summary, an ontology using RDF, RDFS, OWL, SKOS, SHACL and SOIC to illustrate an example of how the support for dependants over their personal and private information might work, would involve several steps and could make use of different vocabularies and ontologies to create a coherent and consistent model that represents the domain, while also being flexible enough to allow for future updates and extensions. The ontology would need to include classes and properties that represent the different parties involved, the personal and private information, the contract and the laws. It should also include relationships that express the *connections between these different components, and constraints that ensure data accuracy and consistency, while also complying with the legal requirements.*

NOTES:

The full description of what the Human Centric AI ecosystem is and how it is intended to work was not provided to the ChatGPT system; therefore, the ontology solution statements were not able to address the specific design related requirements, as that information wasn't provided to it.

Whilst the outline provided by ChatGPT provides some usefully progressive 3rd party input (that was otherwise broadly sought, yet still absent); the details, will take a lot of time and effort to better define as to form some sort of useful specification, for each use case example, which i consider to be a non-trivial (series of) task(s).

However; importantly, rather than defining a database for persons relating to these sorts of requirements - being defined merely as subclasses of `owl:thing` some insight is able to be progressed in-order to support

Community of Practice

What is a 'Community of Practice'?

A Community of Practice is defined in WikiPedia in the following way;

A **community of practice** (**CoP**) is a group of people who "share a concern or a passion for something they do and learn how to do it better as they interact regularly". The concept was first proposed by cognitive anthropologist Jean Lave and educational theorist Etienne Wenger in their 1991 book *Situated Learning* (). Wenger then significantly expanded on the concept in his 1998 book *Communities of Practice* ().

A CoP can evolve naturally because of the members' common interest in a particular domain or area, or it can be created deliberately with the goal of gaining knowledge related to a specific field. It is through the process of sharing information and experiences with the group that members learn from each other, and have an opportunity to develop personally and professionally ().

CoPs can exist in physical settings, for example, a lunchroom at work, a field setting, a factory floor, or elsewhere in the environment, but members of CoPs do not have to be co-located. They form a "virtual community of practice" (VCoP) () when they collaborate online, such as within discussion boards, newsgroups, or the various chats on social media, such as #musochat centred on contemporary classical music performance (). A "mobile community of practice" (MCoP) () is when members communicate with one another via mobile phones and participate in community work on the go.

Communities of practice are not new phenomena: this type of learning has existed for as long as people have been learning and sharing their experiences through storytelling. The idea is rooted in American pragmatism, especially C. S. Peirce's concept of the "community of inquiry" (), but also John Dewey's principle of learning through occupation ().

The Concept of a ‘community of practice’ is considered to be more involved that simply having a ‘community standards’ statement or similar; that has historically been shown to be susceptible to be written or re-written, by project owners to most benefit those authors whilst mitigating risks due to wrongs that may have occurred; and/or, issues that the group leaders have no interest in addressing.

One of the areas of particular interest to me - is to support human rights; including, but not limited to, ensuring equitable treatment of people who contribute useful work, when it is found to be valuable; and to ensure ‘probity’ / support for human dignity; by seeking to protect against acts of ‘intellectual dishonesty’, such as re-writing someone's former work then displacing provenance; as is often motivated by simplified economic concepts employed by lay-people and/or bad actors.

The requirements to address these sorts of ‘community of practice’ considerations; do evolve, but must start somewhere - as is part of the consequence of my writing / doing this work; alongside my means to employ concepts / information - I'm aware of; that supports improved communications.

#socialfabric #ValuesFrameworks

BestEfforts

The Concept of seeking to define a framework around Defining of Best Efforts

The concept of "best efforts" typically refers to an obligation or promise to use a reasonable level of care and diligence in achieving a particular result. It is generally understood to mean that a person will make a good faith effort to achieve the desired result, but does not guarantee that the result will be achieved. "Best efforts" does not require someone to go beyond what is reasonable or to sacrifice their own interests in order to achieve the desired result.

In contrast, behaviour that is intentionally harmful, exploitative, or a willful breach of an agreement of fair dealings would involve a conscious choice to act in a way that is detrimental to others or that goes against the terms of an agreement. This type of behaviour would not be considered to be making a "best effort" to achieve a desired result, as it would be motivated by selfish or malicious intentions rather than a desire to achieve a mutually beneficial outcome.

To expand on my interpretation, "best efforts" refers to an obligation or promise to use a reasonable level of care and diligence in achieving a particular result. This means that a person will make a good faith effort to achieve the desired outcome, but does not guarantee that the result will be achieved. "Best efforts" does not require someone to go beyond what is reasonable or to sacrifice their own interests in order to achieve the desired result. This means that if something goes wrong or the desired result is not achieved, it is not necessarily a breach of the obligation as long as the person has made a good faith effort to achieve the result.

In contrast, mistakes that are made intentionally are different because they involve a conscious choice to act in a certain way, rather than being an unintentional or unforeseen outcome. Intentional mistakes are typically made with the knowledge that they are likely to result in a negative outcome, and may be motivated by selfish or malicious intentions. These mistakes would not be considered to be made in good faith or as a "best effort" to achieve a desired result, as the person making the mistake is acting in a way that is not in line with the goal or purpose of the activity.

Source: Chat.OpenAi.com

Fit For Purpose

Content produced quickly via ChatGPT

When designing tools that form part of an ecosystem's solution that is implemented using software and socio-economic systems; how would you define a rule or condition that a useful component should be 'fit for purpose', define 'fit for purpose'..

The term "fit for purpose" refers to the extent to which a product, service, or system is suitable or appropriate for the specific purpose or use for which it was designed. When designing tools as part of an ecosystem solution that is implemented using software and socio-economic systems, it is important to ensure that each component is "fit for purpose" in order to maximise the effectiveness and efficiency of the overall solution.

To ensure that a component is "fit for purpose," it is necessary to consider a number of different factors. These might include the specific requirements or needs of the users or stakeholders who will be interacting with the component, the technical capabilities and limitations of the component, and any regulatory or compliance requirements that must be met.

Overall, a component is considered "fit for purpose" if it meets the specific needs and requirements of the users or stakeholders, and if it performs the functions it was designed to perform in an effective and efficient manner.

What sorts of considerations should be made to evaluate whether or not a solution meets the specific needs of a particular use case?

There are several considerations that should be made when evaluating whether or not a solution meets the specific needs of a particular use case. Some of the key considerations might include:

1. The specific requirements or needs of the users or stakeholders: It is important to carefully consider the specific needs and requirements of the users or stakeholders who will be interacting with the solution. This might include factors such as the tasks they will be performing, the information they need to access, and any specific constraints or limitations they may face.
2. The technical capabilities and limitations of the solution: It is also important to consider the technical capabilities and limitations of the solution, and to ensure that it is capable of performing the tasks it was designed to perform. This might include factors such as the performance, scalability, and reliability of the solution.
3. Any regulatory or compliance requirements: Depending on the context in which the solution will be used, there may be certain regulatory or compliance requirements that must be met. It is important to carefully consider these requirements and to ensure that the solution is compliant.
4. The cost and value of the solution: It is also important to consider the cost of the solution and to ensure that it provides good value for money. This might involve comparing the cost of the solution to the benefits it is expected to provide, and determining whether the benefits outweigh the costs.

Overall, these are just a few of the key considerations that should be made when evaluating whether or not a solution meets the specific needs of a particular use case.

Learning Modals

How to define Learning?

Learning is the process of acquiring new knowledge, skills, behaviours, or attitudes through experience, study, or training. Learning can take place in a variety of contexts, including in formal educational settings, such as schools or universities, or informally, through life experiences or self-directed study.

There are many different approaches to learning, and people learn in different ways. Some people may learn more effectively through hands-on experience, while others may learn better through reading or listening to lectures.

Learning can be a continuous process that occurs throughout a person's life, as they encounter new situations and experiences that challenge them to learn and adapt. It can also be a deliberate process, as people may seek out learning opportunities in order to acquire new knowledge or skills.

Overall, learning is a fundamental aspect of human development and is essential for personal and professional growth and success.

The Use of Open Badges with HumanCentricAI systems

OpenBadges can be used to provide recognition of prior learning for knowledge workers via systems that support Human Centric AIAI agents in a number of ways:

1. Recognition of skills and expertise: AI agents can be used to assess the skills and expertise of knowledge workers and issue Open Badges to recognize their learning and achievements. This can help to provide evidence of skills and abilities that may be difficult to demonstrate through traditional methods.
2. Verification of learning: Open Badges can be used to verify the learning and achievements of knowledge workers, helping to ensure that their skills and expertise are accurately represented.
3. Portability of learning: Open Badges can be easily shared and displayed on a variety of online platforms, making it easier for knowledge workers to share their learning and achievements with others. This can be particularly useful for knowledge workers who may work in a variety of different settings or who may be seeking to demonstrate their skills to potential employers or clients.

Overall, Open Badges can be a useful tool for providing recognition of prior learning for knowledge workers via systems that support AI agents, helping to provide evidence of skills and expertise and making it easier to share learning and achievements with others.

Objective

The objective is to improve the way people are able to be supported by recognition of prior learning applications of CognitiveAI tooling. These systems will seek to develop an evidence base to support a conclusion that a person can be asserted to have knowledge of concepts, things, fields of expertise and other factors of importance in relation to the performance of new work activities, as is in-turn made possible by the prior performance of activities.

In-part, what this constituency seeks to form a means to address, relates to innovation in particular; but also, an array of other socio-economic and governance factors.

Within the field of innovation, people work on new ideas that form new 'things', of various types. Yet traditional / historical means of qualification have been mostly focused upon the use of academic facilities, which do not offer qualifications about the knowledge of a field that is presently being invented. The consequence is that the people who were instrumental to the creation of a new field of expertise, are subsequently not considered to be qualified in the area and consequentially; both, discriminated against due to not having done a course relating to the field (only available later); and in-turn somewhat forced to pay 'rents' to obtain qualifications for an area that they may have been involved in creating / inventing!.

The commonly accepted solution for this problem is to simply pay the 'rents' or suffer the consequences.

The other area illustrated, about improving ESG support (in-effect); is that projects that are run by groups may in-turn nominate a person to take-on a role that they are not competently equipped to perform; and as a consequence of these sorts of practices, harms may in-turn be incurred by others - that may well be of a kind, that has no appropriate available lawful remedy.

In a similar yet different area; a person may be charged with the responsibility of providing an analysis of a situation and acting or failing to act in a circumstance that has material consequences upon others; but they've not got the skills to comprehend some sort of important facts, due to a lack of skills or knowledge in that area. Consequentially the person may act negligently and/or engage in - what is in-effect - an act of violence, and then seek protection at a later time, irrespective of the consequences put upon others. At which stage, the situation may in-turn become adversarial and the victim is unlikely to be resourced with lawful remedy, compensation and/or even simply an otherwise appropriate apology and whatever further actions may need to take place in-order to resolve the consequences of that person's mistakes; as was in-turn put, upon others. These sorts of situations undermine 'good faith' relations and in-turn often invoke further wrong-doings as the mistakes of one person, may in-turn lead to an array of other persons seeking to cover up and/or protect the wrong-doer, irrespective of whether it was an honest mistake or a willful act of violence causing injury.

So the learning modals, seek to support sense-making to more rapidly produce contextually useful insights and related links that support a means to process the circumstances of a person's learning and seek to mitigate risks of events that may lead to disputes and/or SocialAttackVectors that may negatively impact a legal entities ESG and/or insurability status.

Additionally, the objective is to produce systems that can provide categorised qualification SemWebOntologies and TemporalSemantics that is in-turn intended to support CognitiveAI processes (noting the importance of: HumanCentricDigitalIdentity) and thereby providing support for VerifiableClaims&Credentials in relation to this field of WebScience and its means to address various SocialFactors.

Temporal Semantics

Temporal semantics is a branch of semantics that deals with the study of time and its relation to language and meaning. It is concerned with how time is expressed, interpreted, and understood in natural languages, and with the ways in which time affects the interpretation of words, sentences, and texts.

Temporal semantics is an important area of research in linguistics, philosophy, computer science, and other fields. It has a wide range of applications, including natural language processing, machine learning, knowledge representation, and artificial intelligence.

In natural language, time can be expressed in many different ways, including through words, phrases, and grammatical constructions that denote past, present, and future events.

Temporal semantics is concerned with understanding how these expressions are used to convey temporal information, and with the ways in which this information can be interpreted and used by speakers and listeners.

In addition to studying the temporal aspects of natural language, temporal semantics also investigates the ways in which time is represented and manipulated in computational systems, such as database systems, knowledge bases, and artificial intelligence systems. It is concerned with developing formal models and methods for representing and reasoning about time in these systems, and with the ways in which these models and methods can be used to support a wide range of applications.

The use of 'Temporal Semantics' is critical to the entire ecosystem; and one of many related objectives include employing the techniques to address SocialAttackVectors that employ temporal factors as part of the attack method; alongside, an array of happier purposes for providing support for temporal semantics.

About the Primary Author: Timothy Holborn.

I was involved in defining underlying technologies that are now deployed globally, long before many of those that would subsequently be defined as 'the experts' were at all involved.

When producing open-royalty free patent-pool supported technology standards[78][79] that can be used for any lawful purpose, effectively as a tool. My interest was in producing infrastructure to support the provision of evidence about circumstances of importance, to courts of law, to protect human rights of children, in particular from bad and/or criminal, public sector professionals.

Whilst works and prior designs had broad-ranging implications, primarily via the advancement of works that started in 2000. My maternal grandfather, Dr John P Carew MBBS FRACP, FCPA, FCP (London) was a notable pathologist, his cousin, Sir John Carew Eccles AC FRS FRACP FRSNZ FAA[80] was awarded a nobel prize for his works relating to consciousness.

I considered then, back in 2000, wiring 'online data storage' like a brain, providing a means to send links not documents, for other people to exploit a person's work without fair payment; To

---

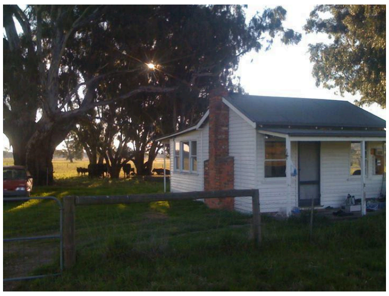
[78] https://www.w3.org/Consortium/Patent-Policy-20200915/

[79] https://www.w3.org/Consortium/Member/List

[80] https://cdn.knightlab.com/libs/timeline3/latest/embed/index.html?source=1r-bo83ImIEjSCmOFFMcT7F79OnCHDOGdkC_q9bOVFZq&font=Default&lang=en&hash_bookmark=true&initial_zoom=4&height=750#event-sir-john-eccles-brain-speech-and-consciousness

form what i first considered as an 'information banking' systems, with the view to addressing simpler use-cases before updating the works, somewhat defined by my uncle, to electronically distribute clinical diagnostic records - as was part of how medical records systems came about.

After the events, the experiences of 2010, seeing the moral decay, irrespective of the infrastructure i'd been involved in putting into data centres and telecommunications exchanges years earlier, abhorrent crimes, amongst the most heinous, in my opinion (indeed, continuing including but not limited to governmental 'social security' systems, still providing false statements); so, back then, made homeless as i was told by respected barristers, that seeking the convention of the rights of the child to be meaningful, was an act considered to be 'tilting at windmills'; irrespective of any such testimonials, by 'honourable persons', i went on a mission, updated works to define a 'knowledge banking' systems (inc: AI, IoT, etc); yet, the notes made about the ***Safe t(ech) net****, relate to some of the intended applications to support via rule of law, human rights and particularly therein, those of children.*



Working from a hut, on a satellite connection provided freely - as I worked both on global issues, as well as working to define telehealth solutions, to improve access to mental health services for children & families… I never imagined the path this would lead my life to take.

Sadly, the consequence of these works from 2010 onwards, irrespective of the successes for others, and in a variety of other areas; has not yet delivered fit for purpose tooling to protect children, in particular whilst certainly not exclusively otherwise. Whilst I am told on an on-going basis, that others, in particular my government, are doing it all already and that there is no useful means to provide any information they do not already know, and that i have not done anything in my life to usefully contribute towards any form of governmental policy[81]*; In-turn, when they have failed, no penalty nor consideration applies, and this is a widespread behaviour demonstrated by many public sector human beings, for gainfully funded activities.*

Yet, when victims need to find some sort of journey out[82]*, they're not safe, indeed the consequence may in-fact be much much worse for those people, which is hard to fathom, but horrifically shown to be true; as mostly women, working in the places, are so very selfish. It was not actually about women's rights or the rights of children, they only care for themselves.*

---

[81] 11/11/2022. 2:23-2:30pm GMT+10, by "Tamzen" on behalf of SA Senator & Foreign Minister Penny Wong.

[82] https://www.youtube.com/watch?v=EV1NFYTwM3k

So, these sorts of experiences, led to better understanding 'dissociative identity disorder' or DID, these experiences, whilst hard to digest, exemplified the requirement for verifiable claims; the means, to form a timeline of electronic evidence, in full, as to define and illustrate; the reprehensible, the reprobates and those who are so much worse.

It is these behaviours that led to the term 'human centric' first being applied upon the works now known as 'verifiable credentials' and/or, in many cohorts, 'digital identity'.

The intended purpose was to create verifiable claims, about what people actually do - to present to courts of law. As such, when i hear the testimonial that the human rights works defined by me, should be redefined to be 'woman centric' rather than human centric, whilst discouraged from illustration the truth about why i termed the intended purpose of the name, in such a way, it says everything about the status of an organisations whose sacred duty, is to uphold the terms outlined on paper, not as a means to create a persons inalienable rights, but rather, in consideration of the time, after the last world-war[83] *that a corpus*[84] *decided to write them down; and to whom, we owe a great debt… lest we forget...*

The implication still remains that the ability to present evidence about reality as is required to benefit those who do good, rather than those who are skilled in the many areas required to be leaders of doing the opposite, is still not part of how their works act, to define people, by design. As such, I assume that the issues illustrated broadly, are already being addressed and that the benefits from this document are more likely to be supportive of other jurisdictions, whilst otherwise noting; that the cost of doing this work, in reality, incurred enormous sacrifice, and that for anyone considering honestly doing this type of thing in future, be aware of the costs, many do not survive and they will not be remembered, as others claim provenance; but moreover, benefit, because what they most want is money, not responsibility.

Australian Law (corporations act) does not easily support means for incorporated entities or their directors, to focus on human rights, particularly in areas of advanced - innovative (truly innovative) new technology R&D. As such, the work was undertaken as a human being, with a business number (as a natural person); and in-turn also, trading names to define the IP structures of works. As a human being, I was able to advocate for use-cases, others did not, though not able to, as a consequence of terms of employment & duties associated with employers. So whilst the personal impacts have been significant, this is effectively the basis upon which my works have been done leading to my relationship, with all connected to it.

---

[83] https://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/

[84] https://www.un.org/en/observances/human-rights-day/women-who-shaped-the-universal-declaration

I seek to continue to act in support of works aimed to deliver outcomes for the betterment of our human family, and through us - our biosphere; in the capacity of being human, seeking to affirm my personal commitments as an honourable person, to commit acts of affirmation towards such ideals. If any questions are raised about the nature of my negative experiences, I can provide 'verifiable claims', but moreover, if there's aspects about my works that are not well known because i didn't publish the works online, then, perhaps the underlying implication of having survived a decade of slavery like governmental treatment, maligned, exploited, abused and worse, all whilst i maintained a clean criminal record, as has always been considered incredibly important for my work, irrespective of what is demonstrated to be provided, furnished and/or engended socio-economic support, to others.

The purpose of my works have been to support rule of law, advancing upon work done first, in a church, in Holborn[85]*, yet this is not what seems to matter as the harms of wrong-doings of others continue to take their toll.. It is nonetheless, a remarkable experience, from the time of supporting AusCivics*[86][87]*, and had a voice via media playing on the public screens at chogm*[88]*, defining the first attempts*[89][90]*, and so much since. Was I the human being who asked the UN to use its instruments to provide terms, for people, required to use electronic contracts*[91]*? idk.*

---

[85] https://www.londonxlondon.com/the-best-things-to-do-in-holborn/

[86] https://www.youtube.com/watch?v=6lasZCwYijU

[87] https://www.youtube.com/@auscivics/videos

[88] https://thecommonwealth.org/charter

[89] https://drive.google.com/file/d/13jjiVON6uodPX3fwoiZbvQ43IjzJnOLc/view?usp=sharing

[90] https://drive.google.com/file/d/1EOTzwJmgJhuFl7uvKhlUwmUO6FcQXd0_/view?usp=sharing

[91] https://soundcloud.com/ubiquitous-au/my-question-human-rights-instruments-for-digital-wallets-valuescredentials