

Social Attack Vectors

Started by: Timothy Holborn NOTES

The purpose of this document and its contents is to produce a series of use-cases pertaining to the different ways people (and their agents) can engage in hostilities, and produce a means to categorise and seek to classify these sorts of circumstances & situations.

The consequential intended benefit and/or purpose, is to then seek to establish 'safety protocols' or technological solutions that can be employed to both identify, address and rectify the issues and the consequence of those issues via the online systems that are used to engage in the behaviours. As it is the case that not all disputes can be resolved 'online', the means for systems to support the requirements of courts of law is considered imperative. This is not with the intent of seeking to have all disputes settled via courts of law, but rather to ensure that parties are empowered to do so, should that be the only reasonable avenue; as would in-turn be assessed and considered by any court of law presented with any such case.

Evidence Standards

There are various standards for evidence that need to be considered when seeking to design appropriate means to support safety protocols that are equipped to support rule of evidence

- [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

Therein, the means to consider how 'safety protocols' can be made to work; first needs to consider the sorts of 'social attack vectors' (as i've termed them); that need to be addressed.

The early 'safety protocols' document can be found via this link;

https://docs.google.com/document/d/1VBBFQbjpXeUad_cgu-3TS67GtXZixA5M9nRdkMDU0Y4/edit?usp=sharing

But this document needs to be redrafted, updated and published as a different document.

Document History

Made available as a google-doc for the purpose of encouraging participatory improvement on the 1st of March 2023. This document has since been developed further as the consequence of works have progressed. 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 webizen systems; although others are encouraged to produce fit for purpose solutions also. Since the initial creation of these documents, international works have been instantiated to create standards, that may or may not end-up being employed via the embodiment of 'webizen' specifically.

The documentation may at times not reflect these changes, due to not having made the alterations needed to reflect the change in circumstance and therein also, audience and intended purpose.

Indeed, some of the reason for the works is to seek to create open-standards to support human rights; rather than seeking to do so via a particular platform. As such, whilst the 'spirit' and 'purpose' of the work has conceptually developed in a consistent manner with the intent; the documentation may not reflect this growth well enough.

The historical 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.

Components of this document refer to the ecosystem that was initially being developed, prior to the works then expanding to support ecosystems more broadly than any single implementation.

As such, there are various references to 'webizen' which pertains to webizen.org which may or may not be employed by the end-users and/or beneficiaries of these works.

Great efforts are being undertaken to seek to produce tools to address humanitarian problems, on a humanitarian basis. The basic needs of all members of our human family should be available for use permissively, and on fair terms, for the benefit of all and in a manner that foundationally acts to support human rights.

Nonetheless; the way these works have developed to become more involved with efforts to produce global standards related works, was unforeseen at the time of the original works.

The Contents in this document is being transferred into a spreadsheet for the purpose of defining an ontology to represent the concepts; [here is the link to that spreadsheet.](#)

Table of Contents

Evidence Standards	1
Table of Contents	3
Introduction	5
Summary	6
ChatGPT Contributions	10
Commercially Motivated Attacks	12
Discrimination based attacks.	15
Unintended Consequences.	16
Dishonesty	16
Cyber Attack Vectors	17
Attacks Online	17
Cyber Crime	18
Social Engineering Attacks	18
Database Attacks	20
DeepFakes	20
Digital Slavery	21
Misrepresentation	26
Nobody AI	26
Tech Debt	27
Permanent Identifiers	29
Strategic Harms & Exploitation	29
Academic / Institutional Funnelling	30
Authorised Thinkers	30
Brain Rape	30
Commercial Exploitation	31
Compromising	31
Dehumanisation	32
Fake News	33
False Attribution	35
Impairment	36
Manipulation	36
You Must Be Famous!!!	36
Agency & Choice	37
Psychological Attack & PsyOps	37
Public Sector Wrong Doings	38
Reversal	41
Social Contract Gamification	41
Temporal Attacks	42
The Harvester	43

"The Secret"	43
Social - Personal (inc. Family Attacks)	45
Torts	45
Outline of tort law	45
Economic Torts	48
Intentional Torts	49
Negligence	49
Nuisance	50
Criminal Activity	51
Summary	51
Corporate Crime	52
Environmental Crime	54
Financial Crimes	54
Fraud	55
Proxy Attacks	55
Ontology related works	56

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 Human Centric AI technology; and that therefore, are amongst the issues that need to be responded to on a Best Efforts basis; to form a Fit For Purpose solution, that is better able to address these sorts of issues than may otherwise be the case.

The considerations include Cyber Attack Vectors 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 Guardianship Relations and related Guardianship Semantics 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 Human Centric AI systems - tell the truth and seek help.

The consideration is not about the person who gainfully harmed others seeking to make payment via 'The Secret' in their pity puddle of their own making; rather, it is to ensure that The Values Project 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 & consequentially 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 The Values Project.

The (formerly termed the Webizen Alliance) and instrumentally therein also; The (Webizen) Charter is intended to be very clear both by statement and consequential technical apparatus, about rendering support for human right and other related Values Credentials.

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 Ecosystems 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 Ecosystemss and related Values Credentials related systems; which are in-turn supported via the Safety Protocols 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,

- Attacks Online
- Criminal Activity
- Public Sector Wrong Doings
- Commercial Exploitation
- Dehumanisation
- Dishonesty
- 'Fake News'
- Temporal Attacks

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

The Values Project seeks to employ various methods, including Web Science and other SocialFactors related considerations to structure methodologies to enable means for people to be better equipped to both benefit from the support of Safety Protocols 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 Trust Factory 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 Freedom Of Thought 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 Web Science); 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 Human Centric Digital Identity 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 Ending Digital Slavery.

*Understanding Ontologies 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 Webizen Tech Stack 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 The Webizen Charter, the Community Of Practice and other Webizen Alliance Commercial Models that as stated - seek to support the growth of the far broader Peace Infrastructure Project , 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 Values Credentials - 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 & 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.

Discrimination based attacks.

NOTE: below text has been initially 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 Criminal Activity 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 Social Attack Vectors 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 Strategic Harms 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.)

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 False Attribution.

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 Ecosystems 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 Safety Protocols for Ending Digital Slavery 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 rudder 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 diminishing 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

<https://drive.google.com/file/d/1cfwFa76HtAUDm22XIQ-FA7buQGYKThOc/view?usp=sharing>

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” 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 tons 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 Criminal Activity 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:

le: 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 Ecosystems 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.²³

Source: [WikiPedia](#)

These sorts of attack vectors require Dishonesty and are closely aligned with Torts, Cyber Attack Vectors, Commercial Exploitation and Criminal Activity. 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, Public Sector Wrong Doings, works to Compromise and engender Impairment whilst delegating Authorised Thinkers who may in-turn be young, yet enthusiastic yet overwhelmingly otherwise - somewhat innocent (and often also - not treated well themselves!).

By funnelling works via False Attribution related tactics into large institutions, the institutions provide a barrier and/or defence framework, that protects any underlying person who is wilfully engaged in Strategic Harms and perhaps also Criminal Activity.

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 Criminal Activity 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 Public Sector Wrong Doings and Commercial Exploitation.

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, Temporal Attacks 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 Temporal Attacks, 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, Attacks Online and Criminal Activity 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 Criminal Activity; 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 Criminal Activity 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 Social Attack Vectors 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 Webizen to 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 Temporal Attacks.

In relation to Criminal Activity and Commercial Exploitation 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 Temporal Attacks and other Social Attack Vectors 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](https://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 include but are not limited to, Plagiarism, Commercial Exploitation, Dishonesty, Fake News 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: Criminal Activity / Financial Crimes) 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 Temporal Attacks 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 Commercial

Exploitation 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 Criminal Activity.

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 Commercial Exploitation.

Blackmailing

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 The Values Project.

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 Knowledge Work 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 Commercial Exploitation.

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 Strategic Harms usually for purposes relating to Misrepresentation and CommercialExploitation.

Psy Ops 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 Freedom Of Thought and engender outcomes that support the objectives of the attackers. These activities are in-effect a form of activity that relates to Digital Slavery.

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...

Reversal

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 Criminal Activity 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 Strategic Harms, although generally also linked with Commercial Exploitation 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 Social Attack Vectors, 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 Freedom Of Thought Safety Protocols requirements.

Not all problems are able to be canvassed in public. There are serious issues that relate to serious Criminal Activity 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 Safety Protocols 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;

- 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.
- 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.
- 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.
- 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 misled 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 Knowledge Work and leads to both Digital Slavery related consequences, which may in-turn become associated with Criminal Activity and/or Public Sector Wrong Doings, 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 The Values Project and in-turn also, The Work Platform.

"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 Social Attack Vectors 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 Guardianship Semantics 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 Temporal Attacks (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, Commercial Exploitation and in-turn both Criminal Activity & Public Sector Wrong Doings.

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 Digital Slavery.

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 Digital Slavery notes, yet others may relate to Mental Illness, Guardianship Relations 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.

Social - Personal (inc. Family Attacks)

There are many different ways a person can be attacked via their social relationships and indeed also, in relation to their family members and/or loved ones.

These attack vectors may relate to efforts that seek to harm a person's social wellbeing, social standing, personal relationships or the lives of loved-ones which thereby needs to be attended to; which provides attackers an opportunity to exploit the engendered situation for gainful purposes.

There are various ways these attacks can be performed. A lot of work needs to be done in this area. It is expected that many different use-cases can be identified and then processed.

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 Deleva, 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 Digital Slavery considerations, alongside those associated with Public Sector Wrong Doings, notwithstanding broader associations with Commercial Exploitation, Criminal Activity, Attacks Online and other Cyber Attack Vectors, Temporal Attacks, 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 Digital Slavery and Dehumanisation issues that are related to Corporate Crime in particular, although not exclusively.

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 .
```