ALL RISE

SAY NO to Cyber ABUSE

The Productivity Commission

Submission: Disruptive Technologies

1st February 2016

The Productivity Commission

1st of February 2016

Submission: Disruptive Technologies

Social Media, Smartphones, Cloud Computing, Email all components of what has been coined 'Disruptive Technologies' – and all part of the overturning of traditional business methods and practices that have the potential to lack refinement and control.

Internet usage is central to a Global economy's digitisation as we enter into the **'Second Machine Age'** or as crowned at the 2016 World Economic Forum in Davos the **'Fourth Industrial Revolution'.**

"**Digital misinformation has become so pervasive in online social media that it has been listed by the World Economic Forum as one of the main threats to human society."** (1) Biased narratives, false beliefs, unsubstantiated rumours, mistrust and paranoia are growing exponentially alongside economic growth in our digital economy.

Whilst technological advancement accelerates and creates opportunity for increased efficiency, growth, jobs and improved consumer accessibility the acceleration is also highlighting the need for action surrounding regulatory and legislative requirements. Mounting evidence cannot be ignored that EVERY Internet device is proving to be a potential open channel for Cyber Crime - Cyber Abuse and EVERYONE now lives with the threat of being a potential target.

A snapshot of statistics below form a disturbing and powerful picture of the impact of what should be read and understood to have the potential utilise such digital platforms as destructive communication.

Cyber Abuse and Cyber Crime is not only systemic but proliferates from the day-to-day experiences of the individual to the largest of corporations with little to no consequence online. A now critical turning point is realised, where the wide-reaching extent of the harm being instigated and created by Cyber Crime – ie: Cyber Abuse, is at times more harmful than physical abuse, impacting our communities both socially and economically on a Global scale.

- Goggle and McAfee estimate there are 2000 cyber attacks every day around the world costing the GLOBAL ECONOMY about £300 BILLION a year. (2)
- Cyber Crime risk moved into the top 5 risks faced by Australian business in 2014 according to Allianz Research – IT WASN'T IN THE TOP 10 IN 2013. (3)
- 90% of Australians worry they will be a victim of online crime (4)

The current All Rise global survey of over 12,500 adult and youth respondents in equal numbers alarmingly reveals thus far:

- 1 in 2 say they have experienced some form of cyber bullying in their lifetime.
- 50% said it led to feeling depressed, lonely or self-harm.
- 68% of those seeing cyber abuse happening to someone else say they did NOTHING about it.

The potential impact of ignoring or remaining to exist in an unregulated environment in the digital landscape can only be further highlighted by the exponential growth in these sectors. This rapid growth whilst bringing immense opportunity also highlights exposure to economic vulnerabilities. Note that:

ONLINE BUSINESS ACTIVITY

New research from Accenture Strategy- a global consulting firm in digital technology has quantified that the digital economy represents one-third of the U.S. economy - equivalent to $5.9 trillion.

According to the same research the proportion is similar in the U.K. and Australia, and falls to about one quarter in France and Germany.

ONLINE PLATFORMS

Platform holders such as Amazon, Uber, Airbnb, Facebook: These brands have reshaped multiple markets by mastering the so-called platform economy, whereby they use the network effects of bringing suppliers, customers and partners together to deliver new forms of value.

Statistics inclusive of: search engines, social media ecommerce platforms, app stores, price comparison websites indicate:

- Over 40% of the world population use the internet
- 3 billion people accessing online platforms.
- Facebook alone has 1.5 billion monthly active users
- Twitter has 1 billion unique visits

The top 15 of these platform players have a collective market cap of $2.6 trillion. European policymakers have expressed concern at their dominance.

Within this, platforms generate, accumulate and control an enormous amount of data and utilise algorithms to convert this into usable information with **90% of all data circulating on the Internet created less than 2 years ago.**

AUSTRALIA AS A CASE STUDY

With the release of the 2013-2014 Communications Report (5) ACMA Chairman Chris Chapman stated, “Consumers are doing more over the internet, using more devices and accessing more online services” – with “growth in these areas posing both opportunities and challenges for traditional industry revenue streams”.

The subsequent 2014-2015 Communications Report states that “Australians are going over-the-top (OTT) with online communications and video services” with almost all adult Australians (94%) having a mobile phone, and there was yet again a massive increase of 85% - in the amount of data downloaded over mobile handsets since the previous year.

The ACMA statistics state that the majority of adult Australians are frequent internet users and access the internet several times a day—**12.2 million (66%) went online three or more times a day as at June 2015.**

- At **June 2014** there were **31.01 million mobile services** in operation **in Australia increasing to** 31.77 million in 2015.
- At May 2015, **13.41 million Australian adults (74 %)** were estimated to **be using a smartphone compared** to 12.07 million (67%) at May 2014.
- The total **volume of data downloaded in Australia** during the June quarter of 2015 was **41% higher** than the volume downloaded during the June quarter of 2014
- 2015- 15.8 million or **86% of Australians have home Internet connection.**
- **92 % of adult Australians accessed the Internet** in the six months to May 2015.
- 2013-2014- Nearly **7 in 10 Australians (68%) are using 3 or more devices** of which -
  - 76% mobile phones;
  - 74% laptops;
  - 67% desktop computers;
  - 54% tablets.

In 2015, Australia had the highest proportion of consumers who had made a contactless tap-and-go purchase (53%), ahead of Singapore (45%), Taiwan (41%) and Canada (37%).

- Australian businesses continued to generate increased economic value from the internet with an estimated $266.8 billion in revenue generated from online sales of goods and services during 2013–14, a $20 billion increase over 2012–13.
- Expenditure on online advertising grew by 16.2% to $4.63 billion over the 2014 calendar year. This represented a 36% share of total media advertising expenditure, compared to 30% in 2013 and 25% during 2012.
- **Four weeks to June 2015, 7.6 million adult Australians (41%) made a purchase or sold something online.**
- In the six months to May 2015, an estimated 13.9 million people (77% of the adult population) went online to conduct banking, pay bills, or buy and/or sell goods and services.

Inclusively Internet security was addressed in the ACMA report stating:
"Growth in the intensity of Australians' online engagement is also matched by an increase in their exposure to network security risks. There was an increase in the average number of computer infections reported under the Australian Internet Security Initiative by participants in 2014–15—averaging 26,645 per day compared to 25,839 in 2013–14."

CYBER ABUSE IS FAR MORE THAN A YOUTH ISSUE

Typically and more prevalently Cyber Abuse (Cyber Crime) has been approached as a youth issue, however more and more both the All RISE survey and engagement with industry experts, businesses at large and with the advent of more legal cases it is being exposed that this is far from being the case.

Initiatives have been implemented in an attempt to address cyber security, phishing and spam issues these are not the only attacks that have a social and economic impact. Cybercrime has been categorised by the Australian Cybercrime Online Reporting Network (ACORN) as:

- Attacks on computer systems
- Cyber bullying
- Illegal and prohibited content
- Online child sexual abuse material

- Identity theft
- Online trading issues
- Email spam and phishing online scams or fraud

It is being reported that ACORN is demonstrating limitations in it's capabilities to address the broad spectrum of Cyber Abuse and Cyber crime that is being encountered with cases referred to the Local Area Police Commands who have not been educated or equipment to handle the sophistication of such attacks.

What has been shown is that this framework, while addressing what should be referenced predominately as Cyber Security issues, the undercurrent of online usage is much more rampant and infectious with behaviours that if enacted upon in a physical environment would be addressed as criminal behaviours. The impact of such an online environment is demonstrating very real life consequences. Addressing such online issues appear to sit outside the remit of regulating agencies to date.

Currently statistics reported by the ACMA on illegal and offensive online content appeared to be limited to dealing with content and investigations of occurrences involving minors and are subsequently transferred to the Office of the Children's eSafety Commissioner. According to the ACMA Hotline for illegal and offensive online content in:

- 2013-2014 - There was an **increase of nearly 550 %** in the number of items of online child abuse and other illegal material referred to law enforcement agencies. The increase is a result of a rising number of complaints to the ACMA.

- 2014–2015, the ACMA received 4,801 complaints (an 18 %increase compared to 2013–14) and finalised investigations into 8,728 items of content as at 30 June 2015

These figures are not to be dismissed as a quarantined 'Youth' issuer as they are reflective and a serious warning that is indicative of the trend of usage that is forming online behaviours. The impact on and from each new generation of users, developers and consumers, unregulated without conscious awareness of the long term consequences, will only further the potential of establishing digital environments that imbed and host a new form of social disease. The subsequent impact can only but flow on from these social behaviours and platforms that will dictate an economic impact.

BUSINESS – THE ECONOMICAL IMPACT

It is evident that the there are many professionals, SMEs and large corporations that are equally experiencing the impact of this 'new age digital revolution', where online usage and behaviours - where Cyber Abuse, Cyber Crime and Cyber Security are drivers of and, have a negative impact on economic viability and development.

With more and more Professionals and Businesses experiencing online targeting, harassment, intimidation, fraud and extortion tactics, manipulation of market power, false reviews, comprise of privacy data, reputational damage, work place bulling and cyber security, the broad spectrum of harm, all of which for them is cyber crime, has very physical consequence. For some companies they do not recover from cyber-attacks and data loss or theft or loss of credibility.

The Internet, whilst providing potential for greater communication within businesses and to market place, is fraught with complexities that have created a fertile and relatively unregulated ground for individuals and companies to enter into unprovoked actions with little or no consequences. Legislative regulation has not kept up with the rapidly changing online environment and subsequently leave very little or no avenue of recourse to address these growing issues.

One Internet SEO specialist company states (and there are more that are echoing similar sentiments) that: *"in the four years to the end of 2015 they have been responsible for the removal of over 2500 defamatory and illegal URL's, which include search engines, social media platforms and websites (average of 10-20 URL's per week)".*

This particular expert goes on to state:

> *"During these four years, I have noticed a significant rise in both the volume of Online Defamation resulting in Reputation Damage and the volume and regularity of related enquiries. At present, we are receiving a minimum of 4 enquiries per week for assistance relating to defamation or illegal actions online. In addition to Newspaper articles, there is now a plethora of consumer review and report forums where users can [without consequence] identify individuals or businesses and cause significant reputation damage.*
>
> *Over the past 18 months, I have recognised an increasing trend in the usage of Internet Review Sites and Social Media Platforms, culminating in increased enquiry for legal and technical assistance by those who are aggrieved.*
>
> *That approximately 1 in 8 clients close businesses due to Internet Defamation and Reputational Damage.*
>
> *Acts such as the TELECOMMUNICATIONS OFFENCES AND OTHER MEASURES ACT (NO. 2) 2004 are rarely utilised or acknowledged by Authorities or Government as being breached by offenders in that a telephone line (internet connection) is being utilised to menace or harass."*

Just one example of the prolific nature of the Internet and the very real damage that result from online abuse.

ABUSE OF THE INTERNET IS NOW RECOGNISED AS AN ESCALATING PUBLIC HEALTH ISSUE

Within digital professions:

- 84% of technology professionals believe there is **real-life risk** and emotional impact for the person being harassed online — most commonly a damaging impact on the victim's reputation (75%) and the potential to influence self-harm (66%).
- More than six in 10 technology professionals think that the tech industry is **not doing enough** to prevent online harassment.
- In terms of possible deterrents and solutions, 75% of technology professionals believe a **universal code of online conduct** would help curb harassment, 51% believe that blocking IP addresses of known harassers would be very effective and 47% believe building more tools into sites to allow users to block or report content would be very effective.
- 90% of tech professionals agree **more tools to block or report** content would have an effect at reducing online harassment

THE NEW TOOL OF WORK PLACE BULLYING AND CYBER ABUSE AT WORK

The risk of experiencing cyber abuse while at work has grown along with the prevalence of companies adopting social media marketing strategies. However, the Facebook, Twitter, Instagram and Pinterest pages of companies have become a playground for individuals who may have personal agendas venting and engaging internally without seemed consequences through to trolls with intent on attacking staff and undermining a brand's reputation. People, groups or other competitors are now free to post comments often with anonymity and without a social filter.

A recent article in the Canberra Times stated that:

- *"Cyber bullies are stalking government workplaces across Australia, exploiting a "cyber underground" where they can harass or intimidate their colleagues with impunity.*
- *A set of three studies involving more than 600 public sector workers from across Australia found* ***72% of participants reported suffering or witnessing cyber bullying at work during the previous six months, with 74% ranking their workplace as highly stressful.***
- *Researcher Felicity Lawrence from the Queensland University of Technology says that even one defamatory video, post or comment had the capacity to go viral, and once posted online could prove hard to remove and could shatter an employee's reputation and career.*
- *With "traditional" workplace bullying thought to cost the Australian economy up to $36 billion a year, Dr Lawrence believes the cost of cyber bullying on productivity could be "profound".*
- *The Queensland University of Technology study found workplace anti-bullying efforts were failing to protect state and federal public servants from web-based harassment and abuse."*

INTERNATIONAL SCENE

Other countries are not immune to the same impact of Cyber Abuse and Cyber Crime that proliferate the Internet and are identifying the growing need to address these issues that are beginning to present as systemic through changes in Legislation.

Acknowledgement by the EU/UK on a Single Digital Market Place identified 'a high level of network and information security and of public safety online across the EU is essential'.

- In the EU 85% of Internet users agree that the risk of becoming a victim of cybercrime is increasing.
- In 2015 - 61% of CEOs state that cyber-threats have become a possible threat to the organisation's growth potential (increase from 48% in 2014).

Currently Online Providers lack comprehensive grievance and remedy mechanisms. There is a considerable gap between what service providers see as sufficient and what user advocates expect where grievances or remedy practices that are in breech of freedom of expression in truth are addressed.

The Global network Initiative (6) has outlined needs to be considered in relation to hosting Platforms and facility engagement via the Internet:

- Due diligence and governance: **According to the U.N. Guiding Principles on Business and Human Rights, governments have the primary duty to protect human rights, but companies have a responsibility to respect human rights.** Companies do not have direct control over the laws, regulations or other government actions of the countries where they operate. However, companies can carry out due diligence to anticipate potential human rights risks, and subsequently make informed business decisions on how to best prevent negative impacts on their stakeholders.
- Grievance and Remedy: **According to the U.N. Guiding Principles, companies should establish a means of identifying and addressing any human rights violations or concerns that occur in relation to the company's business. Internet and telecommunications companies should demonstrate that they have clear mechanisms in place for people to file grievances and receive remedy.** Similarly, users must also have a way of learning about these mechanisms.

NEW ZEALAND AS A CASE STUDY

More Governments are beginning to see, listen and actually experience first hand the impact of allowing the digital environment to remain unregulated. Equalled with this they are hearing and realising the call for action from their Constituents to address and implement necessary and overdue regulation and legislation.

In groundbreaking action the New Zealand Government are now implementing a Law that bans Deliberately Harmful Internet Trolling. Internet trolls who use deliberately harmful, threatening or offensive language could soon face up to two years in jail under the country's new Harmful Digital Communications Bill approved by Parliament recently. (Harmful Digital Communications Act 2015)- (7)

If a person is determined to have posted a digital communication with the intention of causing harm to a victim, they could be fined up to $50,000 NZD ($33,000 USD), while if a corporation causes intentional harm, it faces a fine of up to $200,000 NZD ($134,000 USD).

An article under a parallel amendment to New Zealand's Crimes Act states that a person who tells someone to commit suicide could receive an additional year in prison, even if no suicide attempt is made.

Within the New Zealand framework:

A digital communication should not ...

- *disclose sensitive personal facts about another individual.*
- *be threatening, intimidating, or menacing.*
- *be grossly offensive to a reasonable person in the position of the affected individual.*
- *be indecent or obscene.*
- *be used to harass an individual.*
- *make a false allegation.*
- *contain a matter that is published in breach of confidence.*
- *incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual.*
- *incite or encourage another individual to commit suicide.*
- *denigrate an individual by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.*

The law would also add additional responsibilities for social media sites like Facebook and Twitter. Once a site receives a court order to remove offending content, the Approved Agency is to work with claimants and website owners to have the offending material removed. Failure by site owners to do so could result in $50,000 fines and/or prison terms.

BUT WHAT ABOUT FREEDOM OF SPEECH?

Freedom of speech is often abused in bastardised reinterpretations of Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR). **The Declaration of Human Rights makes it very clear that "Freedom of Speech is not Freedom to Abuse" - that freedom from fear and freedom from harm is paramount as an undeniable human right.** The Declaration states that:

> *1. Everyone shall have the right to hold opinions without interference.*
> *2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
(a) For respect of the rights or reputations of others;
(b) For the protection of national security or of public order (order public), or of public health or morals - and
No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks

ALL RISE OBJECTIVES

ALL RISE is an international not-for profit organisation established for the purpose of calling out cyber bullying, cyber trolling, cyber harassment and cyber stalking for what they truly are – CYBER ABUSE and a CYBER CRIME. **The core objectives of ALL RISE are to Re-define, Educate, Research and legislate,** as needed.

- Glaringly evident from All Rise's already extensive research:
- Awareness of cyber abuse is widespread.
- Committing cyber abuse is easy and relatively free from consequence.
- Cyber abuse has lasting damaging effects on people both physically and mentally. At times worse than a physical beating. It causes real harm to real people.
- Cyber abuse is far from being just a youth issue alone. Every adult knows it occurs, often observes or experiences it themselves, but survives it with 'ignore it and it will go away' attitude.
- Almost all but (only some of) the most extreme cases cyber abuse go unpunished.
- Anonymity is a root concern.
- People struggle in knowing how to handle cyber abuse. It doesn't get spoken about, as people often see it as normal or part of growing up, so people often suffer in silence.
- People often do nothing when they see cyber abuse happening online.
- Some believe free speech means freedom to abuse.
- The current practice of 'ignore it an it will go away' is NOT WORKING.

People want action: the tide of tolerance is turning.

All RISE's own Social Work professional confers:

"*There is a stream of abuse that goes out and another that returns as people attempt to control, coerce and bully those around them.* ***Abuse has become normal currency in social media and appears to be the most traded commodity in the world today.*** *Cyber-abuse is a normal way of life for many and largely accepted as such. The impact on mental health and relationships is far from normal – it is devastating."*

ALL RISE will continue to pursue all avenues and development to ensure the Re-definition, Education Research and Legislation in necessary consultation with individuals, businesses and Governments is enacted. Please do not hesitate to contact us if further comment and consultation is sought in relation to any of the above-sited information.

References:

1. According to research done by Laboratory of Computational Social Science, Networks Department, IMT Alti Studi Lucca, 55100 Lucca, Italy
2. (2) Google and McAfee estimate there are 2,000 cyber attacks every day around the world, costing the global economy about £300bn a year. http://www.bbc.com/news/uk-34622754
3. Cybercrime risk moved into the top 5 risks faced by Australian business in 2014 according to Allianz research; it wasn't in the top ten in 2013. http://www.allianz.com.au/media/news/2014/allianz-launches-cyber-risk-insurance-product
4. 90% of Australians worry they will be a victim of online crime. http://www.qt.com.au/news/new-facts-emerge-about-australians-and-cybercrime/2851037/
5. ACMA commissioned survey, May 2015
6. (https://globalnetworkinitiative.org/principles/index.php)
7. http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html