MA dissertation applying the Guiding Principles to ICT companies

Lucy Purdon

Dear Mr. Addo, Ms Guaqueta, Ms Jungk, Mr. Selvanathan and Mr. Sulyandziga.

I have recently completed an MA in Human Rights at the Institute of Commonwealth Studies in London. My tutor, Dr. Corinne Lennox, suggested I send you my dissertation as it may be of interest and some use for the working group when debating the human rights responsibilities of ICT companies.

Titled: "Privatising Dissent: How do the Guiding Principles on Business and Human Rights apply to ICT Companies?", I have used the issues raised in Frank La Rue's report devoted entirely to the Internet which was presented to the HRC in June 2011 to test the ability of the GPs to be applied effectively to any industry, in this case ICT companies. As this issue of human rights in the digital age is something of a 'hot topic' this year, events changed from day to day and I hope it contains the most up to date examples.

I found the research thoroughly enjoyable and wish you all the best in your mission to uphold and enforce the GPs.

Best regards and many thanks,

Lucy Purdon

Privatising Dissent: How do the Guiding Principles on Business and Human Rights apply to Information and Communication Technology (ICT) Companies?

Student Number: 1040634

MA Understanding and Securing Human Rights

The Institute of Commonwealth Studies, School of Advanced Study, University of London

2nd September 2011

Word Count: 15,481

Privatising Dissent: How do the Guiding Principles on Business and Human Rights apply to Information and Communication Technology (ICT) Companies?

Student Number: 1040634

This dissertation is submitted in partial fulfilment of the requirements for the degree of MA in Understanding and Securing Human Rights at The Institute of Commonwealth Studies, School of Advanced Study, University of London.

2nd September 2011

Word Count: 15,481

CONTENTS

Abstract

Three significant events in 2011 have informed this study: Events known as the "Arab Spring" where protest and revolution has enveloped Tunisia, Egypt, Syria and Bahrain among others with significant attention paid to the role of the Internet; *The Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression*, Frank La Rue and the *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* presented by the Special Representative on the issue of human rights and transnational corporations and other business enterprises, John Ruggie. Using the issues addressed in Frank La Rue's report devoted entirely to the Internet, this study analyses how the Guiding Principles can be applied to ICT companies using examples of situations presented by the Arab Spring and worldwide in order to prevent violations of the right to freedom of expression and the right to privacy on occasions when the Internet is used for human rights advocacy.

I. Introduction

The relationship between business and human rights has been a tense and much debated topic in the human rights realm for many years. Although States are primary duty bearers for human rights, business practice can have a potentially damaging effect on the entire spectrum of recognised human rights. From oil companies to clothing companies, the potential for transnational corporations (TNCs) to commit human rights violations has been well documented in cases such as oil exploitation by Shell in the Niger Delta, the sweatshops of Gap clothing and the diamond mines in Sierra Leone.

In human rights advocacy, the Internet provides an easy and cheap way to communicate and the ability to organise thousands of people; when utilised in recent protests and revolution in the Middle East and beyond, the Internet helped depose authoritarian leaders and provided a catalyst for potentially lasting change. These events turned the human rights spotlight on the business operations of Information and Communication Technology (ICT) companies, which in this study includes Internet Service Providers (ISP), Internet Content Providers (ICP), mobile communications, and hardware and software providers.

Frank La Rue, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, devoted his entire report on access to the Internet, which he presented to the Human Rights Council (HRC) on 3rd June 2011 (UN 2011b). In the introduction to his presentation, La Rue (Introduction I.2., p.4) declared,

"The Special Rapporteur believes that the Internet is one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information, and for facilitating active citizen participation in building democratic societies."[1]

1 . All quotes from La Rue are taken from the report presented at the 17th Session of the HRC on 3rd June 2011 A/HRC/17/27 (UN 2011b).

However, using the Internet for advocacy is not without risk, as La Rue (III.23, p.7) continues,

"At the same time, these distinctive features of the Internet that enable individuals to disseminate information in "real time" and mobilise people has created fear amongst governments and the powerful. This has led to increased restrictions on the Internet through the use of increasingly sophisticated technologies to block content, monitor and identify activists and critics, criminalisation of legal expression, and adoption of restrictive legislation to justify such measures."

It is rare that a State has the necessary knowledge and tools to be able to carry out these actions themselves, so they turn to the private companies that run the online spaces to restrict access, or those which could potentially provide the hardware and software to launch censorship and surveillance operations. As John Palfrey notes,

"In almost every case, States have to rely upon private actors to carry out most of the censorship and surveillance. The means, by which States call upon private actors, and for what purpose, vary from State to State. But the trend points toward greater expectation placed by States on private actors to help get the online censorship and surveillance job done" (Palfrey 2008, p.70).

These actions are violations of the right to freedom of expression and the right to privacy, Article 19 and 17 of the International Covenant on Civil and Political Rights (ICCPR) respectively, which are analysed in this study. La Rue (III.22, p.7) reminds us "the Internet also facilitates the realisation of a range of other human rights"; exercising the right to freedom of expression helps defend other human rights and draws attentions to human rights violations.

On 16th June 2011, a few weeks after La Rue presented his report, the HRC adopted the *Guiding Principles on Business and Human Rights: Implementing the 'Protect, Respect and Remedy Framework'* (Guiding Principles) (UN 2011a), presented by the Special Representative John Ruggie. These Guiding Principles (GPs) are not legally binding but were presented by Ruggie as the "end of the

beginning" (GPs Introduction 13, p.5) signifying the journey to this point of recognition and the work still to be done in the longer term.

Although the GPs were not designed to be sector specific, this study aims to test the relevance and adaptability of the GPs to any area of industry by applying them to ICT companies, using the concerns raised in La Rue's report on State attempts to restrict Internet use by:

- Arbitrary blocking and filtering of [online] content.
- Criminalisation of legitimate expression.
- Imposition of intermediary liability.
- Disconnecting users from Internet access, including on the basis of intellectual property rights.
- Cyber attacks.
- Inadequate protection of the right to privacy and data protection.

An argument on the issue of Internet access would be futile without the necessary infrastructure, so La Rue dedicates the second half of his report to:

- Addressing universal access to the Internet.

From the analysis of these categories and the GPs, the study will close with a chapter on the gaps in protection the research has highlighted. The individual GPs are studied numerically where possible, but they do occasionally intersect and overlap across chapters.

Although this study was inspired by the events of the Arab Spring, it draws on worldwide, current examples to support a balanced argument as this is an issue which affects both authoritarian and democratic States.

i.) Framework and Methodology

There exists an academic argument on the human rights obligations of non-State actors, and an argument of a good Internet versus a bad Internet, but there are no studies specifically on how the GPs can be applied to ICT companies using La Rue's report. The purpose of the study is not to explain the working intricacies of technology, neither is it a study of the sociological aspect of how networks are formed (references to further reading on these topics are provided) but to identify where ICT companies are at risk of committing or being complicit in human rights violations and test them against the weight and relevancy of the GPs. It is hoped this will encourage further specialised application to other industries.

Events surrounding this study are very recent and due to the nature of technology, move very fast. Once the relevant academics in the field were identified and published work reviewed, following them on Twitter became a good source of finding the most up to date information. Certain academics in this field are prolific 'tweeters': Evgeny Morozov in particular along with Ethan Zuckerman of Global Voices and Jillian C. York of Electronic Frontier Foundation. These 'tweets' provided links to primary sources such as newspaper articles, blogs and reports. Non-governmental organisations (NGOs) and academic institutes dedicated to this area release timely reports, ensuring their status as leaders in the field. This study draws on reports by The Berkman Centre for Internet and Society at Harvard University, Open Net Initiative, Reporters without Borders, Human Rights Watch and Amnesty International.

ii) Acknowledgements.

In 2010-2011, I completed internships with Tactical Technology Collective in Brighton, and Witness in New York and would like to thank these organisations for improving my understanding of the topic. I would also like to thank Sameer Padania, director of Macroscope and former Witness manager for agreeing to be interviewed for this study.

II. Background to the Adoption of the Guiding Principles.

There are, "80,000 TNCs operating in the world"[2], 192 United Nation (UN) member States and zero international human rights treaties specifically addressing business and human rights. The UN has made attempts to engage the business community with human rights issues since the 1990s[3] when the private sector rapidly expanded and more businesses operated transnationally. John Ruggie writes in the introduction to the GPs (Introduction 1, p.3), "these developments heightened social awareness of business' impact on human rights and also attracted the attention of the United Nations". It could be argued that the UN may have started to pay attention to the connection between business and human rights due to a number of high profile campaigns and protests by civil society against the business practices of TNCs which jeopardised human rights. Incidentally, some of these campaigns harnessed the organisational abilities of the Internet, which was at that time in its infancy[4]. However, initial attempts to create human rights obligations for business were crushed by the powerful TNCs. The 1990 *UN Code of Conduct on Transnational Corporations* (UN 1990) was never adopted due to corporate criticism that "their human rights obligations under the code would have superseded that of governments" (Hessbruegge 2005, p.45).

While the UN worked on further principles, civil society kept busy. The protests which hijacked the World Trade Organisation's meeting in Seattle in 1999 highlighted corporate failings to respect human rights and were described by Naomi Klein as "the first political movement born of the chaotic pathways of the Internet" (Klein 2002, p.3).

---

2. The quotes continues, "...10 times as many subsidiaries and countless millions of national firms, most of which are small and medium sized enterprises" (GP Introduction 15, p5).

3. The International Labour Organisation (ILO) attempted to address the human rights obligations of business prior to 1990: They drafted the 1977 *Tripartite Declaration of Principles Concerning Multinational Enterprises* which attempted to set out non-binding human rights obligations.

4. The International Campaign to Ban Landmines (ICBL) took advantage of new technology in the 1990s to form a worldwide network pressuring governments to support a ban. This resulted in the patronage of Princess Diana, a 1997 treaty banning landmines and a Nobel Peace Prize for the network and its coordinator. Ironically, the campaign was initiated by a fax (Van Rooy 2004, p.44).

Intergovernmental agencies also tried to link business practice with human rights; the Organisation of Economic Cooperation and Development
(OECD) have their own guidelines, adopted in 2000, the same year the UN launched Global Compact (GC), an initiative which encourages business to voluntarily sign up to Ten Principles spelling out two different types of human rights obligations aimed solely at corporations: not to instigate human rights violations and not to be complicit in violations (Halpern 2008 p.175). To date, the initiative has over 8,700 corporate members from 130 countries. The problem with all these attempts to impose human rights obligations on TNCs is that they are voluntary and self-regulated schemes that have proven, on the whole, inadequate attempts to make TNCs accountable and responsible for human rights. Additionally, there was little or no advice on what corporations should do at an operational level to avoid violating human rights through business practice.

Although some TNCs attempted to engage with human rights, arguably to avoid public relations disasters in the face of gross human rights violations and a growing demand for ethical consumerism, it was not at the forefront of policy. In 2002, Shell published *"Human Rights Dilemmas: A Training Supplement"* which presented a range of situations intended for "group discussion" and "brainstorming" (Shell 2002, p2). Here is an extract from one of the human rights dilemmas:

"You are the General Manager of a Shell operation in a remote area of a country where there is an active rebel force. Public security forces are active in the area, but these forces do not have the resources to respond effectively to rebel activities. Their commander asks if Shell will provide them with some non-military resources, such as transportation, food and other basic supplies. It is made clear that this assistance will be used only in the protection of the company's security. So far, the rebels have not directly affected Shell operations. You decide to provide some of what has been requested but choose not to offer transportation because this could be used in "lethal" armed operations. The commander is pleased with what Shell is willing to provide but asks again for help with transportation, saying that this is for the direct protection of Shell property.

Points to consider:

• How – and by whom – should decisions about responding to such requests be made?

• How – if at all – can Shell determine how the material assistance it provides might be used?

• Are there other ways of responding that might address the situation without involving Shell in government security operations?

• What is the difference between supporting local armed forces for company security and for other, "lethal" activities? Is it possible to identify and differentiate these operations?" (Shell 2002, p.8).

This is clearly a highly sensitive situation which demands a lot more than "group discussion" but it is an indication of the impact a TNC can have on a country, how they can affect the outcome of a political situation and how closely they run the risk of violating human rights. The complexity and nuances of human rights do not appear to be appreciated, along with the consequences of these kinds of actions.

The 2003 *UN Norms on the Responsibilities of Transnational Corporations and other Business Enterprises with Regards To Human Rights* (Draft Norms) (UN 2003) were another attempt to set out international norms for human rights and business. Again, they were strongly opposed by the business community and not supported by the HRC as they were perceived to set out obligations on business which had no grounding in international law and were strikingly similar to the human rights obligations of States (Halpern 2008, p.175). In 2005, the UN created the mandate to appoint a Special Representative for Business and Human Rights, initially for two years, a position held by John Ruggie from 2005-2011. Ruggie distanced himself from the failed Draft Norms and adopted a different approach: he put the views and concerns of business at the heart of his work and spoke the language of business, which appeared to create a more open dialogue and advancement towards agreement of the responsibilities of corporations.

In his 2008 report (UN 2008a) Ruggie presented a single recommendation: to adopt the 'Protect, Respect and Remedy' framework. This was welcomed by the

HRC (UN HRC 2008) which extended the Special Representative's mandate until 2011. This three pillar framework consisted of:

1. The State duty to protect: As primary duty bearers, States must fulfil their duty to protect citizens against human rights violations by corporations.

2. The corporate responsibility to respect: Corporations of all sizes have a responsibility to respect human rights and take steps to avoid negatively infringing on others human rights.

3. Access to Remedy: Judicial and non-judicial remedies. States must ensure access to legal remedies in its courts and companies must have adequate grievance mechanisms.

The 'Protect, Respect and Remedy' framework succeeded where the Draft Norms of 2003 failed as they clearly set out the differences between State duties and business obligations in three distinct framework pillars, therefore avoiding past criticism that business human rights obligations outweighed those of States. In drafting the GPs based on these three pillars, Ruggie consulted hundreds of businesses across all sectors and encouraged businesses to look internally at the human rights they may affect. His office offered help and guidance and encouraged questions and sharing best practice. Of the 100 plus companies consulted in the drafting of the GPs at a multi-stakeholder meeting in Paris on 5th October 2010 (UN 2010), eleven were technology companies[5].

The GPs clearly follow these three pillars in defined sections. GPs 1-10 concern the State responsibility to protect, GPs 11-24 concern the corporate responsibility to respect and GPs 25-31 concern access to remedy. Each GP is accompanied by Ruggie's commentary to clarify interpretation, understanding that business people may not be experts on human rights. Getting The GPs on the table

5 . Representatives from Yahoo!, Microsoft, Nokia, Orange, Hewlett Packard, Symantec, Hitachi, Telefonica (Spain) Telecom Italia, Alcatel-Lucent (France) and Capgemini attended the consultation (UN 2010).

and adopted with the support of the business community[6] is a huge achievement after twenty years of attempts. However, the GPs were designed to be universal and not sector specific, which may make it easier for certain industries to deem them irrelevant, especially as Ruggie declares in the Introduction, "when it comes to implementation, one size does not fit all" (GPs Introduction 15., p.5). At first glance, the GPs could be interpreted as only applying to the activities of TNCs in industries with a bad reputation, such as mining and oil extraction, as although the GPs to do not generally give sector specific illustrations, land rights and labour laws are mentioned and a whole section is dedicated to business operations in conflict zones.

However, Ruggie tackles this problem from the outset of the section on the corporate responsibility to respect. While the jurisprudence of international human rights law is rooted in the relationship between the individual and the State, Ruggie is clear that the GPs apply universally to business in GP 11,

"Business enterprises should respect human rights. This means they should avoid infringing on the human rights of others and should address adverse human rights impact with which they are involved" (II.A.11, p.13).

In case any corporation thought they were exempt, Ruggie spells it out in the commentary,

"The responsibility to respect human rights is a global standard of expected conduct for all business enterprises wherever they operate. It exists independently of States' abilities and/or willingness to fulfil their own human rights obligations, and does not diminish those obligations" (II.A.11, p.13).

Following on from this, GP 12 requires business to *understand* human rights by studying human rights legislation,

6. After the Guiding Principles were adopted, Ruggie received letters of praise and support from, among others, The Coca-Cola Company and General Electric (Global Business Initiative, 2011).

“The responsibility of business enterprises to respect human rights refers to internationally recognised human rights- understood, at a minimum, as those expressed in the International Bill of Human Rights and the principles concerning fundamental rights set out in the ILO's Declaration on Fundamental Principles and Right at Work” (II.A.12., p.13).

The commentary points readers to the main international human rights mechanisms such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Economic, Social and Cultural Rights (ICESR) and the ICCPR adding, “these are the benchmarks against which other social actors assess the human rights impact of business” (ibid).

This chapter has detailed the background to the adoption of the GPs, the format they take and the foundational principles. Before the GPs are discussed in more detail, the next chapter explains the growth of the Internet and ICT companies over the past few decades, alongside some social context and the resulting tensions between corporate and State control of the Internet.

III. The Problem: Who Controls the Internet?

In the early years of the 'dotcom' boom, States imposed little liability or responsibility on ICT companies in order to encourage growth in this emerging industry (Palfrey 2008, p.69). As the Internet became increasingly privatised in the 1990s, young entrepreneurs and technological whiz kids set up companies in their bedrooms or college dorms. One third of the 3,400 Internet companies surveyed in 1999 did not exist in 1996 (Castells 2010, p.151) and the speed at which the industry grew would see some of these companies later be valued at billions of dollars. Manuel Castells (2010, p.152) presents a useful comparison to put this growth into context,

"[In 1999] Yahoo! employing 673 people was valued at $33.9 billion, in spite of meagre quarterly earnings of $16.7 million, in contrast to Boeing, employing 230,000 workers with quarterly earnings of $347 million yet only slightly more valued than Yahoo!, with a market capitalisation of $35.8 billion."

While Castells admits that stocks were "wildly overvalued" (2010, p.152), the industry attracted investment and became "flushed with cash, thus enjoying ample opportunity for innovation and entrepreneurship" (Castells 2010, p.152). However, in 1999, "there was no indisputable, clear authority over the Internet, either in the US or the world- a sign of the free-wheeling characteristics of the new medium, both in technological and cultural terms" (Castells 2010, p.46).

The arrival of Web 2.0 shortly after the turn of the century allowed Internet users to move from being mere consumers to being able to contribute to the shape and content of the Internet, regardless of geography. The Internet recognises no territorial sovereignty or borders adding up to what Castells calls a network society,

"Because networks do not stop at the border of the nation-state, the network society constituted itself as a global system, ushering in the new form of globalisation characteristic of our time" (2010, Preface: xviii).

Although activists had flirted with the Internet's organisational and networking abilities[7] (as mentioned in the previous chapter), it wasn't until the 2009 'Green Revolution' in Iran that the world, and governments in particular, sat up and took notice of the political might of the Internet. When protester Neda Agha-Soltan was shot and killed by a sniper on June 20th, shocking pictures of her dead body were sent around the world, illustrating the brutality of the Iranian regime and disregard for human rights. Dubbed the 'Twitter Revolution' for the site's perceived involvement in organising the protests and disseminating information to the outside world, the press heaped praise on the online tool as the way to topple dictators and bring about revolutions. Evgeny Morozov (2010, p.9) recounts how Twitter was asked by the USA not to conduct site maintenance during the protests; government officials lined up to praise the Internet and a public campaign was launched to nominate Twitter for the Nobel peace prize (Morozov 2010, p.9). Hilary Clinton confirmed the Internet's new 'freedom-fighter' status in a speech on Internet freedom,

"Now, in many respects, information has never been so free. There are more ways to spread more ideas to more people than at any moment in history. And even in authoritarian countries, information networks are helping people discover new facts and making governments more accountable" (Clinton, 2010).

The argument of information equalling democracy is not new. During the Cold War, the USA smuggled photocopiers and fax machines behind the Iron Curtain to enable the spread of copies of samizdat[8] (Morozov 2010, p.7). The collapse of Communism was mistakenly attributed to this increased spread of information, a comparison readily applied today. Replace "authoritarian" with "Communist" and we could be in 1989.

It was seemingly forgotten that in the end, the Green Revolution did not topple a dictator and the government of Iran ultimately tightened control over the Internet, arrested many of the protesters and increased surveillance. When the US

7 "In the 1980s, a former Chilean prisoner of conscience, on whose behalf Amnesty International had campaigned, developed Amnesty's first email system, donating it to the IS [International Secretariat] in appreciation of its efforts" (Lebert 2002, p. 23).

8 .'Samizdat' were copies of censored or banned publications which were photocopied by dissidents and passed by hand from one person to the next.

government asked Twitter to hold off maintenance during the 'Green Revolution', the Internet became politicised (Morozov 2010, p.13) and there were increased concerns about the safety of activists using the Internet for advocacy. The Special Rapporteur on the situation of human rights defenders, Margaret Sekaggya, warned in a report to the HRC that "digital and online security measures should also be put in place wherever possible" (UN 2009a, p.13). Aside from the security implications, journalists such as Malcolm Gladwell (2010) attacked the perceived importance and organisational abilities of social networking sites. In his article *"Why The Revolution Will Not Be Tweeted",* Gladwell questioned the commitment of so called 'clicktavists'[9], bringing the act of protest back to boots on the street, rather than the click of a mouse,

'Once activists were defined by their causes, they are now defined by their tools".

Additionally, for all Clinton's praise for freedom of information, when Wikileaks published cables which exposed the USA's attempts to spy on UN officials, Clinton criticised Wikileaks as "an attack on America's foreign policy interests" (Sheridan, 2010).

History reveals the tense relationship between States and the right to freedom of expression. Paul Gordon Lauren's (2008, p.233) study of the origins of the UDHR reveal China insisted that the article regarding freedom of expression was included in the drafting process. For all the Western democracies rhetoric in defence of the right to freedom of expression, Canada, France, Germany, Italy, and the UK abstained from the vote for the 2008 mandate for Frank La Rue's post of Special Rapporteur (UN 2008b), with a vote from the USA unrecorded. The votes in favour were cast by; *inter alia,* China, Cuba, Egypt, Pakistan, Russia, and Saudi Arabia. This shows the battle to improve the right to freedom of expression is expected to be a complex one.

9 .A 'clicktavist' was described by Micah White (2010) as a trend for activists moving online and applying marketing techniques to activism "Gone is faith in the power of ideas, or the poetry of deeds, to enact social change."

One man's freedom fighter is another's terrorist, and as the political ramifications of the Internet became apparent, States became decidedly more interested in gaining control of the Internet and ICT companies suddenly found themselves in a tricky position. The amount of information held on the Internet about individuals is huge and potentially very valuable for a State wishing to silence its critics. Some States would also be very interested in controlling the amount of information its citizens could access and would also like to keep an eye on critics within its borders. After enjoying many years with little attention from the State, ICT companies were now seemingly complicit with human rights violations, as States turned to private companies to help them violate Article 17 and 19 of the ICCPR and beyond by tracking human rights defenders through their online activities.

Activists must be aware that the Internet is not a free space owned by the people and is becoming increasingly less anonymous. The Internet is a private space run by companies for profit, who hold and control personal information about its users which can be potentially deadly if this information falls into State hands. As Ethan Zuckerman (2010) wrote,

"Hosting your political movement on YouTube is a little like trying to hold a rally in a shopping mall. It looks like a public space, but it's not – it's a private space, and your use of it is governed by an agreement that works harder to protect YouTube's fiscal viability than to protect your rights of free speech."

Examples of human rights defenders using the Internet for activism and being detained or harassed are common; The Committee to Protect Journalists (CPJ, 2009) reported that Burmese blogger Maung Thura is currently serving a 59 year prison sentence for disseminating video footage after Cyclone Nargis in 2008 and a recent survey by Neal Ungerleider (2011) of Harvard University from a pool of bloggers posting to Global Voices from the Middle East showed,

"Seven percent of respondents claimed to have been arrested or detained in the past year, while 30% were personally threatened and 18% had their website or personal accounts either hacked or attacked."

The positive obligations of the right to freedom of expression in Article 19 of the ICCPR, state

"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."

The Internet is the embodiment of these ideas and its founders may have had this precisely in mind when designing the tool that is now inescapable in modern life.

The previous chapters have detailed both the context in which the GPs were adopted and some of the human rights violations associated with using the Internet for advocacy. The next chapters will bring this information together by studying the nature of these violations in more detail, using the issues raised by La Rue, to assess the involvement of the State and ICT companies and applying them to the GPs which may provide a solution to some, if not all, of the problems.

IV. APPLYING THE GUIDING PRINCIPLES:

A. Arbitrary Blocking and Filtering of Content.

While the Internet can be used for human rights advocacy, it can be used in the same way to strengthen authoritarian rule. La Rue (IV.A.29, p.9) identified as his first concern the arbitrary blocking or filtering of content on the Internet. This is the process by which a user is prevented from accessing a particular URL (uniform resource locator) address or domain name outright or certain keywords are blocked from search engines[10]. This is often done for social and political reasons rather than ones of national security. Reporters Without Borders (2010, p.8) stated in its report '*Enemies of the Internet*' that searching the web in China using the keywords 'democracy' or 'human rights' would return zero results. According to Palfrey (2008, p.69), "the most extensive of these filtering regimes are found in States in three regions of the world: the Middle East and North Africa; Asia and the Pacific; and Central Europe and Asia and techniques can vary."

While blocking and filtering of content can be a long-term policy of a State, which violates its duty to protect under international human rights law, La Rue also points out concerns over "just in time" blocking, where users are blocked from accessing information at key political moments such as "elections, times of social unrest, or anniversaries of politically or historically significant events" (IV.A.30, p.9). For example, in July 2011, Amnesty International reported that the Saudi Arabian government blocked access to Amnesty International's website after it criticised a draft anti-terror law that would essentially outlaw peaceful protests.

However, virtually none of the two dozen or so States that filter the Internet have a network controlled entirely by the State (Palfrey 2008, p.70) and rarely have the infrastructure to carry out blocking, filtering or surveillance themselves. States need to enlist the help of private actors who can block and filter content and also develop and sell the hardware and software for a price and therefore a profit.

10. A more detailed technological explanation can be found in Palfrey 2008, p. 72.

This opposes GP 6 (I.B.6, p.10) which is clear that, "States should promote respect for human rights by business enterprises with which they conduct commercial transactions." Instead of encouraging these companies to respect human rights, States are encouraging companies to violate human rights.

In "*How To Do Business With Respect For Human Rights: A Guidance Tools For Companies*" (Global Compact, 2010), a Global Compact (GC) initiative which draws heavily on the Respect, Protect and Remedy Framework, a table spells out a variety of impacts a company can have on human rights. The last in the table is concerned with technology:

Company Function	Positive Impacts	Negative Impacts	Human Rights Possibly affected
Technology	People can communicate and access information	The company sells technology for censorship and surveillance	• Right to freedom of expression • Right to Privacy

Table 1.1 Global Compact 2010, p.36.

This is where we see the tension between State responsibility and corporate responsibility. GP13a (II.A.13a, p.14) requires business to, " Avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts where they occur;". A company providing a service to purposefully block or filter content for an authoritarian regime and one known to violate human rights is not acting within Ruggie's 'respect' framework, essentially the corporate end of the deal. But the GPs go further: 13(b) (II.A, p.14) requires business to,

"Seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts."

This can be interpreted as prohibiting ignorance on 'dual-use' technology to excuse human rights abuse; companies cannot turn a blind eye, no matter the size of the business or the scale of operations. GP 14 (II.A.14, p.14) maintains the "responsibility of business enterprise to respect human rights applies to all enterprises regardless of their size, sector, operational context, ownership and structure."

For example, the technology company Cisco manufacture and sell switchers and routers, which is "Internet backbone equipment" (Castells 2010, p.180). This hardware contains the technological components needed to carry out blocking/filtering, which while used by schools and libraries or to block pornographic content, can also be used by authoritarian regimes to block anything the administrator chooses. Palfrey (2008, p.73) gives an example of dual-use by applying it to nuclear technology, "although nuclear technologies can provide energy efficiently to those who need it, it can also power weapons of mass destruction of previously unprecedented power."

GPs 15 (II.A.15, p.15) and 16 (II.B.16, p.15) require business enterprises to express their commitment to human rights by publicly releasing a statement of policy approved at the highest level and which details operational procedure, "due-diligence" and remediation process. The Business and Human Rights Resource Centre (2011) recorded that out of over 8,700 UN Global Compact members, 289 companies have released a human rights statement of policy which specifically refer to the UDHR as suggested in Guiding Principle 12. Of these 289 companies, twenty are technology or communication companies.[11]

This is an extract from Cisco's human rights statement of policy which appears on their website:

"Cisco does not in any way participate in the censorship of information by governments. Moreover, Cisco complies with all U.S. government regulations which

11 The companies listed are Alcatel-Lucent, BT, Cable and Wireless, Cisco, Dell, Ericsson, Hitachi, Hewlett Packard, Intel, Microsoft, Motorola, Nokia, O2, Siemens, Sumito Electric, Sun Microsystems, Telecom Italia, Vodaphone, Telefonica, Teliasonera (Business and Human Rights Resource Centre, 2011a).

prohibit the sale of our products to certain destinations or to users who misuse our products or resell them to prohibited users.

Some countries have chosen, as a matter of national policy, to restrict or limit access to information on the Internet to their citizens. Functionality inherent in Cisco equipment, such as our routers, may be employed by such nations to restrict this access, but it is important to note that this is the same functionality that libraries and corporate network administrators use to block sites in accordance with policies they establish. This functionality can be used for many different purposes, and Cisco has not specially designed or marketed products for any government, or any regional market, to censor Internet content from citizens.

Cisco cannot determine what sovereign information is regulated by sovereign nations inside their own countries. Even within nations that have signed the UN Global Compact there is rich debate in the courts and society concerning access to the Internet, lines between commercial speech and political speech, and related issues. Cisco supports transparency in the way the Internet is used and complies with all applicable regulations."

The question here is whether Cisco *does* have the power to do more outside of complying with "all applicable regulations". The commentary of GP 11 (II.A.11, p.13) explains that the foundational principle is for business enterprises to respect human right which "exists over and above compliance with national laws and regulations protecting human rights." To apply an example from the pharmaceutical industry, the BBC (2011a) recently reported a decision by Danish drug manufacturer Lundbeck to restrict distribution of an epilepsy drug which has been used to compose a lethal injection to execute prisoners on death row in the USA. While the dual use of the drug is not illegal, Lundbeck has taken steps to ensure it does not legally reach prisons, including an outright ban on distribution to prisons in capital punishment states. Purchasers sign a declaration that the drug is for personal use, it will not be used in capital punishment and will not be re-distributed without the manufacturer's permission. These additional steps by other industries show that turning a blind eye to misuse or dual-use of a company's products is not acceptable by international norms.

States do have to exercise some control over the Internet in order to avoid infringement on other's human rights, in accordance with Article 19 paragraph 3 of the ICCPR which permits curtailment of the right to freedom of expression under these circumstances only if, "provided by law and are necessary:

a) for respect of the rights or reputations of others.

b) for the protection on national security or of public order (*ordre public*), or of public health or morals."

Child pornography and inciting violence are accepted examples, but La Rue (IV.C.31, p.10) raised concerns that even in these instances, States are concentrating on blocking the material rather than investigating the root causes and perpetrators and that "the specific conditions that justify blocking are not established in law or are provided by law but in an overly broad and vague manner, which risks content being blocked arbitrarily and excessively." Blocking lists are kept secret, which makes it even more difficult to ascertain whether blocking is justified under the interpretation of Article 19 paragraph 3.

Now that censorship is the new enemy, the USA has very publicly invested in censorship circumvention technology; Hilary Clinton (2011) included the announcement in her speech on Internet freedom, "We are also supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship." Censorship circumvention is the process by which a user trying to access a blocked or filtered website can access it via a 'proxy' website which looks innocent and has not been flagged by censors.[12] However, censorship circumvention tools tend to be developed by NGOs or not for profit organisations, such as the University of Michigan who are assisting in the development of Telex (Koring, 2011) although Google have also been reported to be investing in censorship circumvention development.

While there was much excitement and investment in these tools as a solution to arbitrary blocking and filtering, recent research has shown the tools have not found the wide audience expected. A study by the Berkman Institute (Roberts et

12 .A more detailed evaluation of censorship circumvention tools can be found in Roberts, et al. 2011.

al.2011) shows that in countries where the most filtering takes place, censorship circumvention tools are not widely used, at most 3%. The study identified several reasons for this: the censorship circumvention tools are slow and/or unreliable[13], they do not allow the user to create content and while accessing international sites without restriction is important, many prefer to utilise local sites. This is where States are winning the battle against freedom of expression. By encouraging the growth of local sites which accommodate language, culture and which are subject to domestic legislation, content can be filtered more easily and they also serve to isolate users from the international community. In doing so, States are not breaking any laws but still controlling the amount of information its citizens can access.

This chapter has shown that the GPs can be applied to the subject of blocking and filtering in that they do not allow business to turn a blind eye to 'dual-use' of products which may violate human rights. This can certainly be applied to ICT companies; if a State cannot block or filter content without the assistance of ICT companies, then they can refer to the GPs to refuse such requests. A wider problem in upholding the right to freedom of expression is the lawful techniques employed by the State to isolate citizens from the international community. The next chapter begins a discussion on how States pass restrictive domestic laws in order to circumvent human rights legislation and restrict ICT companies.

13. Morozov (2010, p.207) detailed the perceived failure of the censorship circumvention tool Haystack, which was removed from circulation in September 2010 amid security fears for activists.

B. Criminalisation of Legitimate Expression

While States can take measures to prevent published information online reaching the end user, La Rue (IV.B.34, p.10) criticises the "application of existing criminal laws to online expression" to prevent publication in the first place. La Rue stresses that "the right to freedom of expression includes expression of views and opinions that shock, offend or disturb" as long as they do not incite violence.

In order for a TNC to operate within a State, they need to obtain a business license and comply with domestic laws. Domestic laws obviously differ from State to State and certain types of information are legal in one country and illegal in another. The most common of these domestic laws include making criticism of State leaders a criminal offence, which violates Article 19 as it does not fall under the terms of Paragraph 3. La Rue (IV.C.39, p.12) cites an example in Turkey, where unlawful content includes ""insulting" the founder of the Republic of Turkey, Mustafa Kemal Ataturk." Freedom of expression on the Internet only exists as a concept if domestic law insists citizens are arrested for expressing an opinion. La Rue (IV.B.34, p.10) continues,

"Such laws are often justified on the basis of protecting an individual's reputation, national security or countering terrorism, but in practice they are used to censor content that the Government and other powerful entities do not like or agree with."

International human rights law mechanisms, such as UN Resolution 12/16 on the Freedom of Expression, proposed by Egypt and the USA in 2009, have attempted to enforce this view, by calling on States to refrain from imposing restrictions on,

"5 (p) (i) Discussion of government policies and political debate; reporting on human rights, government activities and corruption in government; engaging in election campaigns, peaceful demonstrations or political activities, including for peace or democracy; and expression of opinion and dissent, religion or belief, including by persons belonging to minorities or vulnerable groups;

(ii). The free flow of information and ideas, including practices such as the banning or closing of publications or other media and the abuse of administrative measures and censorship;
(iii). Access to or use of information and communication technologies, including radio, television and the Internet."

Reporters without Borders and Human Rights Watch regularly document these instances; Christoph Wilcke (2011) of Human Rights Watch recently reported on a draft amendment proposed in Jordan,

"The government of Prime Minister Maroufal-Bakhitis is doing its bit to stifle free speech in the name of fighting corruption. A draft amendment to a law setting up an anti-corruption agency would punish people who spread "unjustified" rumors about corruption that "lead to insulting the reputation or infringing upon the dignity" of another person, with at least six months in prison... Rather than add new provisions criminalising defamation, Jordan should cancel those already in its penal code that send peaceful critics to jail for "insulting" the king or government institutions."

The timing of this draft amendment is an unsubtle response to the spread of protest in the Middle East, where authoritarian regimes look to stem the flood of criticism of corrupt governments and hang onto power.

In theory, this battle in domestic law about what does or does not constitute legitimate political expression is outside the scope of corporate responsibility as it is not up to the private sector to make laws. However, this is not an excuse to blindly enter foreign markets where it is common knowledge the practice of criminalising legitimate expression exists. Therefore, applying the GPs relevant to the first chapter also apply here. However, this issue is primarily concerned with the harmony of domestic laws, human rights legislation and business practice which is explored in greater detail in the next section.

C. Imposition of Intermediary Liability.

The arrival of Web 2.0 meant that users are no longer solely consumers of the Internet, but can contribute to how the Internet is shaped by being able to publish content without having to go through an editorial 'gatekeeper'. However, it is the case that information is mostly published via private corporations, or 'intermediaries'. La Rue (IV.C.38, p.11) identifies these intermediaries from the private sector ranging from “Internet Service Providers (ISPs) to search engines, and from blogging services to online community platforms.”

The legal protection that these intermediaries enjoyed during the 1990s from liability for content published has been eroded as certain States battle for control of the Internet to prevent corruption, human rights violations and demand for change being made public. As La Rue states in his recommendations (IV.3.74, p.20),

“Given their [intermediaries] unprecedented influence over how and what is circulated on the Internet, States have increasingly sought to exert control over them and to hold them legally liable for failing to prevent access to content deemed to be illegal.”

It is easy to demonise corporations for a seemingly ‘laissez faire’ approach to human rights on the Internet, but a closer investigation of State behaviour shows the pressure companies are put under to comply with State requests that may end in violations of Article 19 and 17 of the ICCPR based on domestic laws. GP 3b (I.B.3b., p.8) calls on States to pass fair laws which enable business to respect human rights,

“Ensure that other laws and policies governing the creation and ongoing operation of business enterprises, such as corporate law, do not constrain but enable business respect for human rights.”

La Rue (IV.C.40, p.12) believes that,

“Holding intermediaries liable for the content created or disseminated by their users severely undermines the enjoyment of the right to freedom of opinion and

expression because it leads to self-protective and over-broad private censorship, often without transparency and the due process of law."

However, in order to protect intermediaries from liability, some States have adopted a 'notice and takedown' policy. This means that instead of being instantly liable for content deemed illegal that is uploaded to the Internet via an intermediary, the intermediary is not liable as long as they remove the offending content as soon as they are made aware of it. This is a problem in the following ways:

1. Intermediaries would be sole decision makers of what is illegal, a provision of the State, and therefore in charge of censorship. La Rue (Recommendation VI.3.75, p.20) maintains that, "…censorship measures should never be delegated to a private entity, and that no-one should be held liable for content on the Internet of which they are not the author."

2. Intermediaries are over-zealous in taking down legitimate forms of political expression.

3. Users are often unaware why their content has been removed.

GPs 18, 19, 20 and 21 address the importance of identifying and assessing human rights risks, assigning responsibility for these risks and track how appropriate and effective the response is to the risks and if/when a business has contributed to adverse impacts, they provide remediation. Corporations must demonstrate a commitment to respecting human rights through a statement of policy and a human rights impact assessment, as suggested by GP18 (II.B.18., p.17), the purpose being to "understand the specific impacts on specific people, given a specific context of operations". To avoid box-ticking, whereby an assessment is done and left on the shelf, Ruggie's commentary to GP 18 suggests,

"...because human rights situations are dynamic, assessments of human rights impacts should be undertaken at regular intervals: prior to a new activity or relationship; prior to major decisions or changes in the operation (e.g. Market entry, product launch, policy change or wider changes to the business); in response to or

anticipation of changes in the operating environment (e.g. Rising social tensions) and periodically throughout the life of an activity or relationship."

This is supported by La Rue (Recommendation VI.3.77., p.21) that corporations should, "continuously review the impact of their services and technologies on the rights to freedom of expression of their users, as well as on the potential pitfalls involved when they are misused." The main way to do this is to adopt a public policy of transparency. Guiding Principle 21 (II.B.21., p.20) states, "In order to account for how they address human rights impacts, business enterprises should be prepared to communicate this externally..." La Rue (Recommendation VI.3.76., p.21) supported this in the recommendations including to "be transparent to the user involved about measures taken."

Google took this literally and from 2010 produces 'transparency reports' which detail government requests for data and traffic flow through the site, which makes it easier to deduce whether a government has interfered with Internet services. The Electronic Frontier Foundation (EFF, 2011) released a report evaluating transparency and privacy practices of popular ICT companies, with Google at the top, earning almost the full four gold stars:

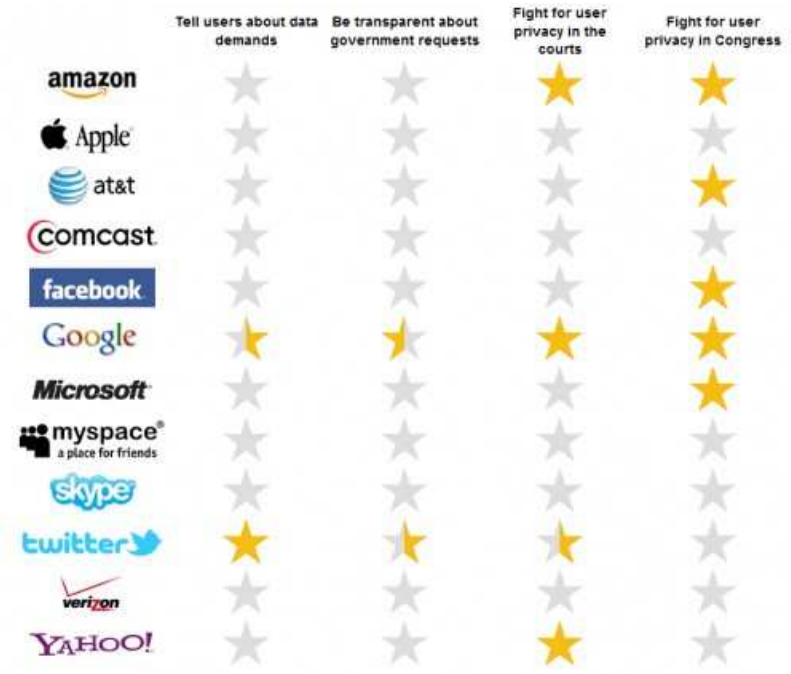

Table 1.2 EFF 2011.

As can be seen from this table, ICT companies are mostly not transparent about the information they share or defend the right to freedom of expression.

In addressing the issue of context, GP 23 (II.B.23., p.21) states that,

“In all contexts, business enterprises should:
a) Comply with all applicable laws and respect internationally recognised human rights, wherever they operate;”

It appears here that the GPs do not appreciate the tension between the State and business as detailed earlier, but it goes on,

“b) Seek ways to honour the principles of internationally recognised human rights when faced with conflicting requirements;

c) Treat the risk of causing or contributing to gross human rights abuses as a legal compliance wherever they operate.”

Ruggie's commentary (II.B.23., p21) clarifies this,

“Where domestic context renders it impossible to meet this responsibility fully, businesses enterprises are expected to respect the principles of internationally recognised human rights to the greatest extent possible in the circumstances, and be able to demonstrate their efforts in this regard.”

This could be interpreted that when intermediaries are faced with “conflicting requirements”, international human rights obligations should 'trump' domestic laws. This gives intermediaries a legitimate reason to refuse State demands which may lead to human rights violations, as long as intermediaries have followed the earlier GPs by putting in place the resources and policy which address human rights in business practice. GP 23b both encourages States to bring domestic laws in line with international human rights legislation and encourages business to bring human rights into their operational framework. It is a very clever inclusion by Ruggie which shows he understands the reality of a TNC’s operations.

Where the GPs are not explicit enough, La Rue suggests multi-stakeholder initiatives can support companies dealing with the nuances of their industry. The Global Network Initiative (GNI) is a collaboration of companies, academics and NGOs which exists to support ICT companies in relation to the human rights landscape. However, only three corporations, Google, Microsoft and Yahoo! have become members so far. Twitter refused to join (Morozov 2010, p.23) citing that they do not regulate content at all and Facebook claimed in 2009 that "as a start-up, our resources and influence are limited" (Forbes 2011). The GNI provides direction and guidance to companies on how to respond to government demands to remove, filter, or block content, and how to respond to demands to disclose personal information to law enforcement agencies, giving companies more of a voice and legitimate reasons to refuse State demands (GNI, 2009). However, with only three corporations and five empty seats on the board, the GNI's influence is questionable.

The concept of transparency involves all corporations undertaking a huge policy shift, investing resources, and perhaps a leap of faith, to put human rights at the forefront of their business practice, however the combination of the GPs, the GNI and Google's attempts will hopefully pave the way in convincing other ICT companies to follow suit.

This chapter has shown the complex problem, multi-dimensional aspects and the push-pull situation between domestic law, human rights obligations and the State-business nexus. Ruggie has given both State and business an incentive to put human rights at the forefront by creating the need of impact assessment and transparency in order to enjoy GP 23, which would give ICT companies a legitimate reason to refuse State demands for user information under domestic law. In turn, this encourages States to bring their domestic law in line with their international human rights obligations. Even though the GPs are meant to be a "coherent whole" and not sector specific, there are unique aspects to each industry sector that require further interpretation of the GPs. Even though the GPs are strong, the question is whether

they can work as a standalone document or need back up in the form of stakeholder initiatives such as GNI. If so, the GNI must be strengthened by convincing more of the powerful technology companies to join forces.

D. Disconnecting Users from the Internet, Including on the Basis of Intellectual Property Laws.

In addition to blocking and filtering measures, La Rue (IV.D.49, p.14) expressed concern over States employing a "centralised 'on/off' control over the Internet." At the height of recent protests in Egypt, the Internet was cut off entirely and during protests in the Chinese province of Xinjiang in May 2010, the Internet was cut off for ten months (Reuters 2010).

However, when it comes to intellectual property (IP) laws, La Rue is concerned by proposals to cut off Internet access to those who violate IP rights. Violating IP rights can come in the form of posting copyrighted content (such as a TV show) to YouTube, or downloading and sharing a song or movie without paying for it. When copyrighted material began appearing for free on the Internet, it took a while for the entertainment industry (film, television and music) to both feel the financial effects and lobby politicians for change. Sameer Padania, director of Macroscope, explains,

"I think the red herring in my opinion is freedom of expression. Freedom of expression is definitely a key issue, but the problem is the Internet companies will hang onto the coat-tails of that issue and will ensure that it is the issue that gets prominence…it's the most visible, the least ruinous intersection they have...there's a whole host of issues the technology companies would much rather we didn't look at in great detail."[14]

Commenting on the title of this study, Sameer asks, "Who is doing the privatising? At the moment it's the creative industries that are holding the whip." Successful lobbying by the entertainment industry has resulted in the blocking of websites containing copyrighted material and disconnection for users violating IP. To use the UK as an example, the Digital Economy Act (DEA) has seen its first success for the entertainment industry in the case of British Telecom (BT) vs. The Motion Picture Association (MPA) (2011), whereby BT have been ordered to block

14 .All quotes with Sameer Padania taken from an interview conducted by the author on Friday August in London. Transcript on file with the author.

the file-sharing site Newzbin2, which collects material already published on the Internet and makes it available for download.

Understandably, ISPs are unhappy about being dragged through the courts and made to block websites or cut off paying subscribers. While a site can only be blocked or a user disconnected from the Internet via a court order (as in the UK), this ruling sets a dangerous precedent and will encourage the entertainment industry to invest more in blocking and disconnecting rather than forming sustainable business models in the new digital landscape. Legitimate political expression often falls foul of copyright laws. Padania notes that, "a lot of political expression gets taken down automatically because they are commenting on a video someone has made a copyright claim to."

Furthermore, BT is using the software Cleanfeed to block Newzbin2, the same software it uses to block child pornography sites. Using the technology in this way is missing the point of the problem. Peter Bradwell, copyright campaigner with Open Rights Group said in a BBC (2011b) interview, "If the goal is boosting creators' ability to make money from their work then we need to abandon these technologically naive measures, focus on genuine market reforms, and satisfy unmet consumer demand."

Rewriting laws restricting Internet use, punishing users and disregarding the consequences goes against the entire concept of the GPs corporate responsibility to respect. States must not pander to business wants as opposed to the human rights of its citizens. While States must pass laws which protect IP, they must not be pressured by commercial lobbies into making laws which ultimately violate human rights. Morozov (2011) is dramatic in predicting the consequences, "All of these proposals are likely to trigger unintended consequences- increased surveillance, stalled innovation and disruption of Internet architecture."

In this case of Business Vs Business rather than State Vs Business, Guiding Principle 8 (I.B.8., p.11) calls on States to assist harmony by ensuring "policy coherence":

"...at times, States have to make difficult balancing acts decisions to reconcile different societal needs. To achieve the appropriate balance, States need to take a

broad approach to managing the businesses and human rights agenda, aimed at ensuring both vertical and horizontal domestic policy coherence".

The application of international human rights law is a 'vertical' one between the individual and the State, but as the balance of power increasingly changes in the world, there is room for a 'horizontal' application between non-state actors (in this case corporations) (Hessbuegge 2005, p.26). For example, several years ago, YouTube enjoyed protection from the USA Digital Millennium Copyright Act which stated it was unnecessary to pre-screen uploaded footage for possible copyright violations. Furthermore, Google (which owns YouTube) assisted users in finding copyrighted content which could be viewed/downloaded for free, frustrating the creative industry and resulting in a number of high profile court cases. However, deals have recently been struck between YouTube and copyright holders which allow copyrighted material to be uploaded and the copyright holders to place adverts around their content. Google have also finalised revenue-sharing deals by creating a program Content ID. James Robinson (2011) explained how Content ID works,

"[Content ID] scans the Internet for pirated material. Content producers can then decide whether to remove those pages or leave them untouched and advertise against them; if they choose the latter option they pocket all the associated revenue."

However, as Morozov (2011) points out, "Do we really want to build tools to screen online content for copyright violations, only to discover that dictators use those very tools for spying on dissidents?"

This is a battle of the giants which is long from over. Online services are here to stay, whether organising protests, buying the weekly shop or watching the latest blockbuster. Disconnecting users from the Internet must be a last resort under any circumstances and disconnection for violation of IP is disproportionate. The entertainment industry has been slow to adapt to the challenge of the digital landscape and are punishing users for it. Industries must find ways to work with the Internet, not against it. The GPs have recognised the challenge of horizontal policy coherence and this must be worked on further in order to avoid infringement of the rights to freedom of expression. ICT companies must adhere to the responsibility to

‘respect’ and avoid using their considerable financial and lobbying resources to push for measures which are disproportionate to the crime.

E. Cyber Attacks.

A cyber attack is an attempt to disrupt the function of a website by hacking or, more commonly, a DDoS (distributed denial of service) attack. A DDoS attack crashes a targeted website by flooding the web server on which it is hosted with requests; the site cannot cope and becomes inaccessible. La Rue (IV.E.51, p.14) noted that human rights activist sites are increasingly the victim of cyber attacks, which are relatively easy to target as the sites are mostly not encrypted and activists rarely have the resources to fend off a cyber attack. Berkman Institute research (Faris et al. 2011, p.7) found that DDoS attacks are "common against independent media sites" and of the sites consulted, 81% who had suffered a DDoS attack had also suffered "at least one other instance of filtering, intrusion or defacement" which suggests evidence of a deliberate and motivated attack, but it can be difficult to prove whether this is sanctioned by the State (via an intermediary as outlined in II.A of this study) or another non-State actor, such as individual hackers. However, if the attack falls around occasions which La Rue describes as 'just in time' or Margaret Sekkagya describes as 'seasonal', the attacks are most likely actions of the State in order to suppress the right to freedom of expression. In the wake of the Arab Spring protests, a Moroccan activist website Manfakinch! (which translates as We Won't Give Up!) suffered a sustained DDoS attack which rendered the site inaccessible for several hours on July 31st 2011 (Global Voices 2011), the same day protesters marched to demand change during a traditional annual ceremony where regional representatives pledge allegiance to King Mohammed (Reuters 2011).

While ICT companies can assist in carrying out cyber attacks, there are companies who are in the business of exposing cyber attacks. ICT security companies are uncovering major instances of cyber attacks, and the perpetrators are often authoritarian States. A recent report by McAfee (2011) details the five year investigation of Operation Shady RAT (this is the acronym for Remote Access Tool but shows even cyber security companies have a sense of humour) identifying 71 targets including governments, companies, the UN and small NGOs, all compromised by a single perpetrator. While the perpetrator is not explicitly named in the report, there are clues,

"The interest in the information held at the Asian and Western national Olympic Committees, as well as the International Olympic Committee (IOC) and the World Anti-Doping Agency in the lead-up and immediate follow-up to the 2008 Olympics [in Beijing] was particularly intriguing and potentially pointed a finger at a State actor behind the intrusions, because there is likely no commercial benefit to be earned from such hacks" (McAfee 2011, p.6).

In a separate report, tracking company Akamai reported Burma as being responsible for 13% of all cyber attacks in the world for the first quarter of 2011, despite only 2% of the population having access to the Internet, which again points to State violations. (Asia News 2011). Companies like McAfee and Akamai have decided to come onto the other side of the fence and reveal government practice, which is commendable but more businesses should be encouraged to step up and help solve these problems by improving tools to deal with cyber attacks and promote human rights. The Berkman Institute (Faris et al. 2011, p.9**)** reported,

"With the adoption of an "Internet Freedom Agenda" by the US State Department, a new pool of money has appeared to support this work. But the most powerful potential allies in a battle for an open Internet are still mostly on the sidelines. Companies like Google, Facebook, Amazon, Akamai, Microsoft and others have resources that could be marshalled to the benefit of Internet users and publishers in closed societies: bandwidth capacity that could support circumvention systems, DDoS-resistant hosting that could protect publishers; technical expertise that could fend of domain hijacking and intrusion. Helping these companies come off the sidelines and bringing them into the game is a key challenge for the future of free speech online."

The GPs encourage business to go "over and above compliance with national laws and regulations protecting human right" (II.A.11, p.13). ICT companies need to be encouraged to use their expertise to actively promote human rights. By separating the State duty to protect and the corporate responsibility to respect, the structure of

the GPs gives business the framework and freedom to form operational policies to do this.

The previous sections of this chapter have mostly been concerned with Article 19 of the ICCPR, the right to freedom of expression and information. The following section is primarily concerned with Article 17 of the ICCPR, the right to privacy which is a much debated and complex issue, but interconnected with the right to freedom of expression because, to quote La Rue (IV.F.53, p.15), “the right to privacy is essential for individuals to express themselves freely.”

F. Inadequate protection of the right to privacy and data protection.

Browsing the Internet was traditionally a space of anonymity, a space where users do not have to reveal their identities and often use pseudonyms when contributing content, something that is being increasingly eroded for both legitimate and non legitimate reasons. According to Article 17 of the ICCPR, States must protect the right to privacy,

"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks."

Under Article 4 of the ICCPR, States are permitted to derogate from Article 17 only "in time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed..." States can put individual Internet users under surveillance to combat terrorism, child pornography or track those inciting racial hatred or imminent violence. But La Rue (IV.F.54., p.15) observes, "While such ends can be legitimate under international human rights law, surveillance often takes place for political, rather than security reasons in an arbitrary and covert manner." An Internet user may have no knowledge of being under surveillance; giveaway signs such as a click on a bugged telephone line or being physically followed do not exist in cyberspace. Intermediaries collect a huge amount of user data that the user may not be aware of, due to inexplicit privacy declarations. Dr Tanya Notley (2011) of Tactical Technology Collective recently commented,

"The problem is that while new communication technologies have become cheaper and easier to use, they have also become more opaque. There are concerns about who owns data when it's uploaded on or created using a commercial service; there is confusion about default privacy settings; and there is the issue of whether individuals are able to control traces of sensitive information they or others leave behind."

La Rue continues (IV.F.54, p15),

"For example, States have used popular social networking sites, such as Facebook, to identify and track the activities of human rights defenders and opposition members, and in some cases have collected usernames and passwords to access private communications of Facebook users".

As part of a wider crackdown on the Internet, access to Facebook was blocked in 2007 (Reuters 2007) by the Syrian government.[15] In February 2011, the site was unblocked. This may appear on the surface a positive response to the wave of change sweeping the Middle East and that Syria responded to the demand for a more open system of government. However, in the space of a few months, it became clear that unblocking Facebook was a tactical move by the Syrian government in order to spy on and entrap its citizens. Jillian York (2011) wrote,

"First came the reports of activists and non-activists being detained, their Facebook and other passwords demanded by authorities for the purpose of monitoring accounts and spying on contacts...the government appears to be handing users fake SSL [Secure Socket Layer- the process which identifies and ensures secure transactions between web servers and browsers] certificates on the HTTPS [secure] version of their site in order to conduct a man-in-the-middle attack and get hold of users' personal information."

Intervening in private correspondence in this instant is a violation of Article 17 (2) and companies such as Facebook are stuck in the middle, having to comply by the terms of their business license to operate in a territory but at the same time suffering what could be determined as hacking. However, Facebook in particular are silent when it comes to this issue, something which lets down the GPs as companies are seemingly complicit. Morozov (2010, p.100) comments,

"The West excels at building and supporting effective tools to pierce through the firewalls of authoritarian governments, but it is also skilled at letting many of its

15 . Syria has declared a 'state of emergency' since 1963 when the Baath party took power in a coup.

corporations disregard the privacy of its users, often with disastrous implications for those who live in oppressive societies."

The Internet holds a huge amount of user information that certain States would love to obtain. La Rue (IV.F.56, p.15) refers to a,

"…worrying trend of States obliging or pressuring these private actors to hand over information of their users. Moreover, with the increase of cloud-computing services [accessing files and applications online instead of downloading them to a computer], where information is stored on servers distributed in different geographical locations, ensuring that third parties also adhere to strict data protection guarantees is paramount."

However, La Rue (ibid)) also admits "...there are insufficient or inadequate data protection laws in many States stipulating who is allowed to access personal data, what it can be used for, how it should be stored and for how long..." ICT companies have in the past buckled to government pressure to provide private information about their users as the law is unclear and conflicting. As more and more people use the Internet, data protection laws need to be under constant review, as Ruggie suggests in the commentary for GP 3 (I.B.3., p.8),

"It is equally important for States to review whether these laws provide the necessary coverage in light of evolving circumstances and whether, together with relevant policies, they provide an environment conducive to business respect for human rights."

Ruggie suggests "greater clarity in some areas of law and policy" (ibid) which is clearly needed in this complex and changing issue, much as in the case detailed earlier regarding intermediary liability.

However, there are some instances where privacy laws are adequate and ICT companies need to employ common sense as opposed to looking to the GPs. For example, Google has experienced much controversy over the issue of privacy.

It was revealed that the cars which collect images for Google Streetview also collected Wi-Fi information from unencrypted accounts, including passwords, email addresses and login names. The BBC (2011c) reported that in May 2010, Google admitted that it had accidentally gathered more than 600GB of this data in more than 30 countries, including the UK. In March 2011, Google was fined 100,000 Euros by France's privacy watchdog CNIL (ibid) and Google Streetview has since been suspended in cities in India, Greece and Zurich over privacy and security concerns. These countries launched thorough investigations into a breach of privacy laws and the UK was criticised for not fining Google, but admitted it had not carried out a very thorough investigation and therefore had no grounds for fining (ibid). In this instance, the UK could be deemed to have failed in its responsibility to protect under the GPs by allowing ICT companies to violate domestic privacy laws.

It could be argued that it seems obvious that a tool such as 'face recognition' software may have sinister overtones, but it has increasingly been integrated into civil society for our perceived social convenience and invested in by ICT companies. Face-recognition technology is commonly used by police, whereby a photo of a suspected criminal is covertly taken and compared in the database.

The service on Facebook that allows users to 'tag' photos of friends has recently been upgraded; while tagging photos, Facebook automatically 'suggests' the name of the person in the photo. This service is provided by an application from a small company Face.com; by tagging one friend, the application will automatically search the whole site to identify other photographs of that person. By 2010, 9 billion photographs had been scanned by the application, identifying 52 million people (Morozov 2010, p.153). It could be argued that recent activity by the Syrian government on Facebook suggests they may have used this application to identify and arbitrarily arrest protesters. Germany has also questioned the application's legality on the grounds the company is “collecting a private database of faces” (BBC 2011d) and Hamburg's information commissioner, Dr Johannes Caspar, stated in a BBC interview (ibid) that, "the risks of such a collection of biometric data is immense." The risks are alarming and if allowed to continue, the technology will only improve and possibly gain acceptance in mainstream opinion.

Morozov (2010, p.154) gives the example of the Smartphone application Recognizr [sic], developed by two Swedish software firms which "allow anyone to point their mobile phone at a stranger and immediately query the Internet about what is known about this person (or, to be more exact, about this person's face)." Google has since decided not to release a face-recognition search engine currently in development for reasons given by Eric Schmidt, the Executive Chairman, that "people could use this stuff in a very, very bad way, as well as in a good way" (The Economist, 2011).

This section has shown that both the State and business have failed in the duty to protect and the responsibility to respect the right to privacy. The GPs do offer some guidance on the importance of policy coherence and the need to review policies in the ever changing environment of technology; this is especially relevant to ICT companies in terms of data protection and privacy. However, where there are adequate privacy laws, ICT companies must constantly review the power of their own products and assess the risks to human rights.

The next section looks at practical case studies to illustrate how the State and ICT companies must understand the other's environment of politics and technology and work together to share best practice.

V. The Pitfalls of Commercial Alignment with Revolution and Political Understanding of Technology.

Google is the popular villain of this story. With annual revenues of $30 billion and an 85% share of the search market (Robinson, 2011), Google's many products and services permeate our everyday lives. Google manages to tick all of La Rue's concerns over human rights violations while being pressured by governments, hated by entertainment industry lobbyists and viewed with suspicion by civil society groups, but is still one of only three members of the GNI and somehow still manages to get it wrong, calling into question the effectiveness of the GNI.

Google ceased operation in China in March 2010 citing the restrictive censorship laws which was "lauded as a bold move to support human rights" by politicians (Morozov 2010, p.21). However, operating in China was damaging the brand not just because of perceived complicity in human rights abuses, but complying with heavy censorship laws meant that when 'Googling' a sensitive term, such as Nobel Peace Prize winner and Chinese dissident Liu Xiaobo (sentenced to eleven years for expressing his opinion of the government on the Internet (Reporters Without Borders, 2011, p.11)), the search would return no results, deeming the Google service irrelevant. Being hailed as revolutionaries for pulling out of China, (Morozov 2010, p.23) was a convenient smokescreen as it covered an embarrassing business failure to launch the brand and a misunderstanding of the politics in a new territory. With 384 million Internet users in China (Reporters without Borders 2011, p.8) it is likely Google will make another attempt to enter the market in the future.

Former Google employee Douglas Edwards recalled in an interview (Adams 2011),

"When Google started, our obstacles were mostly other corporations- Yahoo or whoever. Those obstacles could be overcome with superior technology. But when the obstacle is, say, China, it is a different order of challenge. I think they [Google]

have now understood that there are limits to where the application of cleverness can get you, some problems that technology cannot solve."

At the height of the protests in Egypt, British company Vodaphone was asked to shut off mobile communications, which it did arguing that it had to comply with government orders under the terms of its operating license agreement. Not only that, it agreed to send out pro-government text messages to its customers on behalf of the government,

"The Armed Forces ask Egypt's honest and loyal men to confront the traitors and criminals and protect our people and our honour and our precious Egypt" (Riley, 2011).

Post-revolution, Vodaphone's marketing company JWT released a promo video entitled 'Our Power' with images of the protests in Tahrir Square and the tagline "We didn't send people to the streets, we didn't start the revolution … We only reminded Egyptians how powerful they are" (Shenker, 2011).

This caused obvious outrage among Egyptians and around the world, prompting Vodaphone to distance itself from the promo claiming it had no knowledge. The video has since been removed from YouTube and other news sites, but not before websites like www.ihatevodaphoneegypt.com sprang up. Vodaphone released a human rights policy statement in 2009, which is published on the Business and Human Rights Resource Centre. The statement explains the company did not join the GNI as the initiative was deemed more relevant to Internet providers (Vodaphone 2009), which shows a lack of foresight as to how their own technology might affect human rights.

2011 has been a defining year for social unrest. Whether a response to decades of authoritarian rule or the effects of economic collapse and austerity cuts, most countries have experienced some kind of social unrest, both in the Global North and the Global South. At the time of writing, England was surveying the physical and

social damage from the worst riots seen for decades. While the use of social media has been praised for helping mobilise people in legitimate political protest, the uglier side of the same tools became apparent as they were allegedly used to coordinate looting during the London riots; this time the target is BBM (Blackberry Messenger). BBM quickly allows the user to instantly message groups (one-to-many) even when there is no mobile phone signal and all for free, unlike PAYG (pay as you go) texting. Using BBM is not like posting to social networks as it is encrypted, a feature which appealed to the original target consumer: business. After the 'Facebook Revolution' and 'Twitter Revolution' in the Middle East, BlackBerry must be deep in its own Cobra meeting on how to avoid the BlackBerry Riots/BlackBerry Mobs moniker (Purdon, 2011).

While corporations can be naïve about the workings of politics, States can be naïve on the workings of technology. RIM (Research in Motion, who own BlackBerry) have stated they will "cooperate fully" (Kunet, 2011) with authorities and David Cameron has planned a review of social media policies, including shutting down social networks in situations such as the recent riots. A meeting is scheduled for home secretary Theresa May to meet executives from Facebook, Twitter, RIM and the Metropolitan Police which is reported to last all of one hour (Halliday, 2011).

Referring to the GPs, a company can avoid a knee-jerk reaction by a State in a situation like the recent riots, by operating within the domestic boundaries of law. Plans to bar certain people from using social media displays a naivety and misunderstanding about how technology actually works. This is why transparency, as strongly advocated in the GPs, is so important. From situations like these, it is clear how a misunderstanding about how technology actually works could lead to damage to business. It is in an ICT company's interest to be transparent about how their product works, the risks involved and how they can be tackled.

Technology may have helped organise looting in this instance, but almost as quickly has helped police catch those who committed crimes. Greater Manchester and Devon and Cornwall police force both stated social networks had an "overwhelmingly positive" role in dispelling rumours and reassuring residents during

the riots" (Halliday, 2011). The 2005 riots in France, which took place when social media was in its infancy, lasted three weeks and resulted in 9,000 cars set on fire in 250 towns and cities across France (Henley, 2011) and were not the product of the organisational abilities of social media. Those who are experts in the field of technology are not concerned with these knee-jerk reactions to Internet services. Sameer Padania says,

"It's easy to make comparisons of what happened in Egypt and Syria, but those are police States, those are human rights abusing states that don't have democratic systems of accountability and authority, they don't have proper governments, they don't have systems of recourse, the companies operate in a very different way in those spaces, I mean look at Vodaphone, they rolled over like a puppy, so it's a different thing here, there are systems here..."

Cutting off the Internet during the revolution in Egypt did not result in everyone going home. Cutting off social networks in times of 'social unrest' will set a dangerous precedent. The UK must be careful what it condemns abroad and condones at home; the UK does have the legal mechanisms to prevent actions that may happen elsewhere and though corporations do have to adhere by domestic laws, if the GPs hold enough weight and put human rights at the forefront, GP 23b may help to avoid these situations in countries where domestic laws are not as strong. Unsurprisingly, the UK government has decided to drop plans to block social media sites. It seems the one hour meeting was enough.

VI. Access to Remedy and Gaps in Protection.

i.) Access to Remedy

The last section of the GPs concern the third pillar of the framework: access to remedy. GP 25 (III.A.25., p.22) is the foundational principle that when abuses occur, those affected have access to effective remedy "through judicial, administrative, legislative or other appropriate means." When it comes to violations of freedom of expression or the right to privacy, access to remedy may not be as clear as say, an oil company who has physically polluted an environment and rendered it uninhabitable. As discussed in previous sections, attributing a violation to the freedom of expression by an ICT company can be difficult to prove.

Legal grievances between businesses, such as ISPs and the entertainment industry as mentioned earlier are expensive and lengthy affairs and are governed by corporate law rather than human rights law. Ruggie's efforts to bring human rights law into the landscape have been discussed.

In terms of individuals or communities whose human rights have been violated, court cases against large TNCs have been brought to the US courts under the Alien Tort Claims Act (ATCA), a law passed by the first Congress in 1789 and lay dormant for over 170 years. This law allows foreign nationals to bring cases to the US courts concerning violations of customary international law. Since 1980, cases have been brought against corporations under the ATCA including Del Monte, Chevron, Royal Dutch Shell, Rio Tinto, Talisman Energy, Occidental Petroleum, Eastman Kodak, Texaco, Exxon, Unocal, Freeport McMoRan, Coca-Cola, Gap, Unocal and Pfizer (Halpern 2008, p.166). For small and medium sized businesses who want to engage with human rights, these high profile, aggressive cases did not encourage asking questions about best practice for human rights which reflects the importance of putting in place non-judicial remedies. Cases against technology companies brought under the ATCA concern ISP Yahoo! and technology company Cisco, both brought by Chinese human rights activists.

In 2007, Yu Ling, the wife of jailed Chinese dissident Wang Xioning, brought a case under the ATCA against Yahoo!, claiming that pro-democracy essays Wang had distributed via a Yahoo! email account were handed over to the Chinese

authorities by the corporation, resulting in Wang receiving ten years in prison on charges of subverting State power. In the same year, journalist Shi Tao also received a ten year sentence for contributing to an Internet forum on media censorship, also through a Yahoo! account. As with most cases brought under the ATCA, the case was settled out of court for an undisclosed sum (Business and Human Rights Resource Centre, 2007).

In 2011, two separate cases were filed against Cisco (Business and Human Rights Resource Centre, 2011b),one by the group Falun Gong and one in Maryland, USA, on behalf of three Chinese dissidents. They both concern the Golden Shield Project, a system developed by Cisco which the plaintiffs claim was used to track Internet activity, identify anonymous bloggers and arbitrarily detain them. In the case of the Falun Gong movement, some members disappeared or were killed. The case is ongoing, but Cisco denies any involvement, saying this software is sold around the world, which reflects the human rights policy statement mentioned earlier.

These cases are long, expensive and the issue of accountability is very difficult to prove. How could it be proved that Cisco knowingly supplied software to the Chinese authorities which would be used to arrest and kill dissidents, or that Yahoo! did hand over user details to Chinese authorities? These actions are kept secret, blocking lists are not published and it is difficult to prove who is the perpetrator of a cyber attack. In the report '*Grievance Mechanisms for Business and Human Rights: Strengths, Weaknesses and Gaps'* in many countries, “legal recourse is not a credible option” (Rees 2008, p.8).

The GPs are vague in the issue of remedy and it is difficult to apply them to ICT companies in practice; Ruggie's commentary (III.A.25., p.22) suggests that “Remedy may include apologies, restitution, rehabilitation, financial or non-financial compensation and punitive sanctions (whether criminal or administrative, such as fines), as well as the prevention of harm through, for examples, injunctions or guarantees of non-repetition.”

Some ICT companies do not display very obvious grievance mechanisms. For example, Facebook’s online form to submit a grievance only applies to intellectual property infringement and there does not seem to be any other channel of contact.

Multi-stakeholder initiatives such as the GC, GNI and OECD can assist by enforcing their own guidelines alongside the GPs, but Rees (2008, p.9) points out,

"The Global Compact sees its grievance process as primarily a means of generating a response from a company for a person who raises a concern, rather than as a fully-fledged complaint process that follows a grievance through to resolution."

This reflects the sprawling nature of ICT companies and the fact that merely getting the company to respond to a grievance is considered an achievement. For any GNI grievance mechanisms to be effective, they need to have more members of the ICT community signed up. Following the GPs regarding transparency would also assist in this issue and may keep ICT companies out of court if they have in place effective non-judicial remedies.

ii.)Addressing the issue of universal access to the Internet.

La Rue's final point in his report concerns physical access to the Internet. If access to the Internet is a fundamental part of the right to freedom of expression, then campaigning for a free Internet is futile if States do not invest in the necessary infrastructure. For developing countries, La Rue (V.60., p.17) believes Internet access is the key to economic and educational development to prevent a "digital divide." There are practical difficulties in achieving this such as an unreliable electricity supply and access to computers. This is where technology companies can exercise a positive form of globalisation and responsibly invest in a country's network and infrastructure. As mentioned earlier, governments repeatedly misunderstand how technology works and ICT companies should share their expertise to ensure harmony between government policy and reality. Actions like this would also, of course, create a new nation of customers. Business can be a force for good, so giving them positive obligations as opposed to negative would be beneficial.

This study has detailed the problems associated with mobile phone companies alongside Internet companies. For some developing countries, mobile phones are a much more popular tool for disseminating information but there is no mention of this in La Rue's report. In terms of protecting the right to freedom of

expression and the right to privacy, mobile phone companies must come under the same banner, as detailed in the example of Vodaphone.

It is also important to mention the responsibility of civil society to be aware of the way technology works. By no means are all bloggers dissidents and the State can also use ICTs for their own disruptive means by spreading propaganda and disinformation. This is not illegal and Internet users must exercise their own judgement and learn how to use the Internet safely, in the same way we learn how to cross the road safely by not stepping out in front of an oncoming vehicle.

VII. The Future of the Guiding Principles

John Ruggie's mandate ended with the adoption of the Guiding Principles on June 16th 2011. HRC Resolution 8/7 established a working group on business and human rights, "consisting of five independent experts, of balanced geographical representation, for a period of three years, to be appointed by the HRC at its eighteenth session." The eighteenth session for the HRC will take place from 12th-30thSeptember 2011 and nominations for the working group closed on July 31st 2011. The Working Group will ensure good practice between business and governments and conduct country visits and maintain regular contact with multi-stakeholder initiatives, which as shown in this study is essential for implementing the GPs.

In a statement following the end of his mandate, John Ruggie (UN 2011c, p.2) called for the GPs to be embedded into practice and for international legal standards to be clarified. He warns, "The GPs will be new, at some risk of misinterpretation, and in need of mainstreaming into organizations and disseminating globally".

As technology moves so fast, it is difficult to predict what tools will exist in the future and how they will be used, or even what legislation will be passed to control them. Considering that YouTube is barely a decade old and has grown from a simple site into a billion dollar TNC, and the online community growing every day, the next years are crucial and a huge policy shift is necessary. Perhaps we shall see the rise of more localised services to reflect language and culture and avoid a complete western dominance of the industry, which is why it is in ICT companies' interests to invest in more localised grievance mechanisms and communication. As Morozov (2010, p.100) commented,

"The future of Internet control is thus a function of numerous (and rather complex) business and social forces; sadly many of them originating in free and democratic societies."

This study has shown that even though this may be true; these free and democratic societies are contributing to restrictions.

VIII. Conclusion

The Internet has permeated every area of our lives in a relatively short time and all actors concerned- States, ICT companies, creative industries and civil society- have struggled to keep up with the related human rights problems, especially concerning the right to freedom of expression and the right to privacy. Civil uprisings in 2011 have thrust ICT companies into the spotlight and often left them flailing when confronted by human rights abuses. The work done by John Ruggie since 2005 has infiltrated debate around business and human rights and getting a document both on the table and adopted is a huge achievement. On first reading of the GPs, it may be hard to see how they apply to ICT companies, but hopefully this study has shown just as much consideration must be given to the ICT sector as other more publicly viewed 'risky' business' like oil and textiles . When read in context with a number of other relevant guidelines, such as Frank La Rue's report, the reports of the Special Rapporteur for human rights defenders Margaret Sekkagya and multi-stakeholder initiatives like GNI and the GC, the GPs are on the whole complimented and offer ICT companies a practical framework of how to embed human rights into business practice. The GNI must now address its weaknesses and actively implement the GPs alongside the new working group.

There is undoubtedly still tension, a push and pull between State and corporate responsibility and obligations; the GPs identify this and demand more legal clarity in domestic laws to guide TNCs operating in many countries. Hysterical reactions and unworkable policy from States and business regarding Internet control is not the way forward as the Internet cannot be controlled in the way these actors would like. States must accept the Internet as a channel of communication and fulfil their legal obligation to protect; ICT companies must use their power responsibly and legally and the entertainment industry must accept the Internet is here to stay and instead of trying to control and restrict it, work with it and develop new ways to do business, much as happened throughout history with technological developments like the printing press and the cassette player. In order for violations to be remedied, transparency is the key and a more open policy of grievance mechanisms and remediation is needed to bring the huge ICT companies back down to earth and into the communities and political landscape in which they operate. Putting human rights

at the forefront of business and away from all the political noise is the first step towards dispelling this tension.

The GPs show that respecting human rights is not necessarily a hindrance and in some cases can assist decision making where domestic laws are confusing or fail. The future of the GPs hinges on whether the working group can take this endorsement and popular feeling and push it through to implementation and perhaps eventually, into international human rights law.

Word Count: 15,481

Bibliography:

Primary sources:

Adams, T., 2011. I was Google employee No.59 and lived to tell the tale. *The Observer News Review*, 31st July, p20-21.

Amnesty International, 2011. Amnesty International Website Blocked in Saudi Arabia. *Amnesty International Website*, [online] 25th July. Available at: http://www.amnesty.org/en/news-and-updates/amnesty-international-website-'blocked-saudi-arabia'-2011-07-25
Last accessed 29th August 2011.

Asia News, 2011. Myanmar: Cyber War: Myanmar leader in attacks in 2011. *Spero News* [online] 29th July. Available at: http://www.speroforum.com/a/57871/Myanmar---Cyber-war-Myanmar-leader-in-attacks-in-2011
Last accessed 1st September 2011.

BBC, 2011a. Virginia executes Jerry Jackson amid death-drug row. *BBC News: US and Canada*, [online] 19th August. Available at: http://www.bbc.co.uk/news/world-us-canada-14579136
Last accessed 29th August 2011.

BBC 2011b. BT ordered to block Newzbin2 website. *BBC News: Technology,* [online] 28th July. Available at: http://www.bbc.co.uk/news/technology-14322957
Last accessed 29th August 2011.

BBC, 2011c. France fines Google over Streetview data blunder. *BBC News: Technology* [online] 21st March. Available at: **http://www.bbc.co.uk/news/technology-12809076**
Last accessed 29th August 2011.

BBC News, 2011d. Germans question Facebook tagging privacy. *BBC News: Technology* [online] 3rd August. Available at http://www.bbc.co.uk/news/technology-14391788
Last accessed 29th August 2011.

Business and Human Rights Resource Centre, 2007. Case Profile: Yahoo! Lawsuit (re China) [online]. Available at: http://www.businesshumanrights.org/Categories/Lawlawsuits/Lawsuitsregulatoryaction/LawsuitsSelectedcases/YahoolawsuitreChina
Last accessed 1st September 2011.

Business and Human Rights Resource Centre, 2011a. A List of companies with a human rights statement [online]. Available here:
http://www.business-humanrights.org/Documents/Policies_
Last accessed 29th August 2011.

Business and Human Rights Resource Centre, 2011b. Case profile: Cisco System lawsuits (re China) [online]. Available at:
http://businesshumanrights.org/Categories/Lawlawsuits/Lawsuitsregulatoryaction/LawsuitsSelectedcases/CiscolawsuitsreChina
Last accessed 29th August 2011.

Clinton, H. 2010. Remarks on Internet Freedom. *The Newseum, Washington, DC* [online] January 21. Available at:
http://www.state.gov/secretary/rm/2010/01/135519.htm
Last accessed 1st September 2011.

Cisco, 2011. Citizenship Governance- Human Rights policy statement [online]. Available at:
http://www.cisco.com/web/about/ac227/ac111/cisco_and_citizenship/human_rights.html
Last accessed 29th August 2011.

Committee to Protect Journalists (CPJ), 2009. 10 Worst Countries to be a Blogger. *CPJ* [Online] Available at:
http://www.cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger.php
Last accessed 29th August 2011.

The Economist, 2011. Anonymous no more. You can't hide-from anybody. *The Economist* [online] 30th July. Available at:
http://www.economist.com/node/21524829
Last accessed 29th August 2011.

Electronic Frontier Foundation (EFF), 2011. When the government comes knocking, who has your back? *EFF Deeplinks blog* [online] 22nd April. Available at:
https://www.eff.org/pages/when-government-comes-knocking-who-has-your-back
Last accessed 1st September 2011.

Faris, R. Roberts, H. Palfrey, J. York, J. Zuckerman, E. 2011. "The Evolving Landscape of Internet Control." The Berkman Institute of Internet and Society. [Online] Available at:
http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Evolving_Landscape_of_Internet_Control_2.pdf
Last accessed 29th August 2011.

Forbes, 2011. Why no one will join the Global Network Initiative. *Forbes* [online] 30th March [online]. Available at:
http://www.forbes.com/sites/larrydownes/2011/03/30/why-no-one-will-join-the-global-network-initiative/
Last accessed 29th August 2011.

Gladwell, M., 2010. *Why The Revolution Will Not Be Tweeted*. The New Yorker [online] October 4th 2010. Available at:
http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell
Last accessed 29th August 2011.

Global Business Initiative, 2011. News Archive. *Global Business Initiative* [online] July 25th and 26th. Available at:
http://www.global-business-initiative.org/News.html
Last accessed 1st September 2011

Global Network Initiative, 2009. Global Network Initiative Principles. [Online] Available at: http://www.globalnetworkinitiative.org/principles/index.php
Last Accessed 29th August 2011.

Global Voices, 2010. Syria: Facebook and YouTube unblocked, among others. *Global Voices* [online] 8th February. Available at:
http://globalvoicesonline.org/2011/02/08/syria-facebook-and-youtube-unblocked-among-others/
Last accessed 29th August 2011.

Global Voices, 2011. Morocco: Activist website sustains DdoS attack. *Global Voices* [online] 3rd August. Available at:
http://globalvoicesonline.org/2011/08/03/morocco-militant-website-sustains-ddos-attack/
Last accessed 29th August 2011.

Google, 2011. Transparency Report. *Google* [online]
Available at:
www.google.com/transparencyreport
Last accessed 29th August 2011.

Halliday, J., 2011. Networks to stand firm over government calls for censorship. *The Guardian*, 25th August, pp 16-17.

Halpern, I. 2008. Tracing the Contours of Transnational Corporations' Human Rights Obligations in the Twenty-First Century. 14 *Buffalo Human Rights Law Review* p129.

Henley, J., 2011. Striking parallels between UK riots and France 2005 unrest. *The Guardian* [online] 14th August. Available at:
http://www.guardian.co.uk/uk/2011/aug/14/uk-riots-france-2005- parallels?CMP=twt_gu

Last accessed 29th August 2011.

Hessbruegge J.A., 2005, Human Rights Violations Arising From Conduct of Non-State Actors,11 *Buffallo Human Rights Law Review* 2005 p21.

Hope D.A, 2011. *Protecting Human Rights Online.* BSR [online] February. Available at:

http://www.bsr.org/reports/BSR_Protecting_Human_Rights_in_the_Digital_Age.pdf

Last accessed 29th August 2011.

Koring, P., 2011. How the West is arming the anti-censorship movement. *The Globe and Mail*, 12th August [online]. Available at:
http://www.theglobeandmail.com/news/world/americas/how-the-west-is-arming-the-anti-censorship-movement/article2128588/
Last accessed 29th August 2011.

Kunet, P., 2011. RIM to turn in Blackberry-using looters after the London riots. *The Register* [online] 8th August. Available at:

http://www.theregister.co.uk/2011/08/08/blackberry_riots/

Last accessed 29th August 2011

Mcafee, 2011. Revealed: Operation Shady Rat [online]
Available at:
http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf
Last accessed 29th August 2011.

Morozov, E., 2011. Why the best things in life aren't free. *The Guardian*. 21st August pp 36-37.

Notley, T 2011. Why digital privacy and security are important for development. *The Guardian 'Poverty Matters Blog'* [online] 4th August. Available at:
http://www.guardian.co.uk/global-development/poverty-matters/2011/aug/04/digital-technology-development-tool
Last accessed 29th August 2011.

Palfrey, JG. 2008. Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet. *Harvard Law School Global Information Technology Report World*. MIT Press, Pages: 69-78

Purdon, L. 2011. The heroes and villains of London town. The Blog of Rights [online] August 10th. Available at:
http://theblogofrights.wordpress.com/2011/08/10/the-heroes-and-villans-of-london-town/
Last accessed 1st September 2011.

Reporters Without Borders, 2010. Enemies of the Internet- Countries under Surveillance. *Reporters without Borders* [online]
Available here:
http://en.rsf.org/IMG/pdf/Internet_enemies.pdf
Last accessed 29th August 2011.

Reuters 2007. Syria blocks Facebook in Internet crackdown. *Reuters, US edition* [online] 23rd November. Available at: http://www.reuters.com/article/2007/11/23/us-syria-facebook-idUSOWE37285020071123
Last accessed 29th August 2011.

Reuters 2010. China restores Internet to Xinjiang. *The Guardian*, 14th May [online]. Available at: http://www.guardian.co.uk/world/2010/may/14/china-restores-internet-access-xinjiang
Last accessed 29th August 2011.

Reuters 2011. Thousands protest on Moroccos king's allegiance day. *Reuters, US edition* 31st July [online]. Available at: http://www.reuters.com/article/2011/07/31/us-morocco-protests-idUSTRE76U2CI20110731
Last accessed 29th August 2011.

Roberts, H. Palfrey, J. Zuckerman, E. 2011. Circumvention Tool Evaluation. *The Berkman Institute of Internet and Society.* [Online.]
Available at: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2011_Circumvention_Tool_Evaluation_1.pdf
Last accessed 29th August 2011.

Robinson, J., 2011. Google: Let's make profits, not war. *The Guardian.* 22nd August pp 1-2.

Rees, Caroline. 2008. "Grievance Mechanisms for Business and Human Rights: Strengths, Weaknesses and Gaps." *Corporate Social Responsibility Initiative, Working paper No. 40*. Cambridge, MA: John F. Kennedy School of Government, Harvard University.
Available at: http://www.reports-and-materials.org/Rees-Existing-grievance-mechanisms-Jan-2008.pdf
Last accessed 29th August 2011.

Riley, T., 2011. Shedding light on Vodaphone's digital darkness. *New Statesman* [online] 26th July. Available at: http://www.newstatesman.com/economy/2011/07/vodafone-egypt-telecoms
Last accessed 29th August 2011.

Shenker, J., 2011. Fury over advert claiming Egypt's revolution as Vodaphone's. *The Guardian* [online] 3rd June. Available at: http://www.guardian.co.uk/world/2011/jun/03/vodafone-egypt-advert-claims-
Last accessed 29th August 2011.

Sheridan, M.B., 2010. Hillary Clinton: WikiLeaks release an 'attack on international community.' *The Washington Post* [online] 29th November. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112903231.html

Last accessed 1st September 2011.

TechJournal South, 2011. Two new data breach bills introduced in the Senate. *TechJournal South* [online] 29th July. Available at: http://www.techjournalsouth.com/2011/07/two-new-data-breach-bills-introduced-in-the-senate/
Last accessed 29th July 2011.

UK Digital Economy Act 2010. (c.24), London: HMSO
Available at:
http://www.legislation.gov.uk/ukpga/2010/24/pdfs/ukpga_20100024_en.pdf
Last accessed 29th August 2011.

UN General Assembly 1966, *International Covenant on Civil and Political Rights*, 16th December 1966, 2200A (XXI). Available at:
http://www2.ohchr.org/english/law/ccpr.htm
Last accessed 1st September 2011.

UN General Assembly 1990. *Code of Conduct on Transnational Corporations.* A/RES/45/186 1st December 1990. Available at:
http://www.un.org/documents/ga/res/45/a45r186.htm

Last accessed 29th August 2011

UN Economic and Social Council 2003, *Norms on the responsibilities of transnational corporations and other business enterprises with regards to human rights* E/CN.4/Sub.2/2003/12/Rev.2 26th August 2003. Available at:
http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G03/160/08/PDF/G0316008.pdf?OpenElement

Last accessed 29th August 2011.

UN General Assembly 2008a. *Protect, Respect and Remedy: a Framework for Business and Human Rights.* A/HRC/8/5**,** 7 April 2008. Available at:
http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G08/128/61/PDF/G0812861.pdf?
Last accessed 29th August 2011.

UN Human Rights Council 2008b. *Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* Human Rights Council Resolution 7/36 28th March 2008. Available at:
http://ap.ohchr.org/documents/E/HRC/resolutions/A_HRC_RES_7_36.pdf
Last accessed 29th August 2011.

UN General Assembly 2009a. *Report of the Special Rapporteur on the Situation of Human Rights Defenders, Margaret Sekaggya. Human Rights Council 18th Session.* A/HRC/13/22. 30th December 2009. Available at:
http://www2.ohchr.org/english/issues/defenders/docs/A.HRC.13.22.pdf
Last accessed 29th August 2011

UN General Assembly 2009b. *Egypt, United States of America: Draft resolution 12/16 Freedom of opinion and expression.* Human Rights Council 12th Session. A/HRC/12/L.14/Rev.1. 30 September 2009. Available at: http://daccess-dds-ny.un.org/doc/RESOLUTION/LTD/G09/161/50/PDF/G0916150.pdf?OpenElement

Last accessed 29th August 2011.

UN 2010. Mandate of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and other Business Enterprises. *Consultation with Business Stakeholders on the Implementation of the UN 'Protect, Respect and Remedy' Framework*. Summary Note, 5th October 2010.
Available at:
http://www.business-humanrights.org/media/documents/report-from-ruggie-business-consultation-paris-5-oct-2010.pdf
Last accessed 29th August 2011.

UN General Assembly 2011a. *Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. A/HRC/17/31 21st March 2011.
Available at:
http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.31_en.pdf
Last accessed 29th August 2011.

UN General Assembly 2011b. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue.* Human Rights Council 17th Session A/HRC/17/27. 16th May 2011. Available at:
http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
Last accessed 29th August 2011.

UN General Assembly 2011c. *Mandate of the Special Representative of the Secretary-General (SRSG) on the Issue of Human Rights and Transnational Corporations and other Business Enterprises . Recommendations on follow up to the mandate.* 11th February 2011. Available at:
http://www.business-humanrights.org/media/documents/ruggie/ruggie-special-mandate-follow-up-11-feb-2011.pdf
Last accessed 29th August 2011.

Ungerleider, N. 2011 7% Of Arab Bloggers Have Been Arrested: Harvard Survey [online] 4th August. Available at:
http://www.fastcompany.com/1771520/survey-7-of-arab-bloggers-have-been-arrested

Last accessed 29th August 2011.

Vodaphone 2009. Balancing national security and law enforcement with privacy and human rights. *Vodaphone* [online] 15th October. Available at:
http://www.vodafone.com/content/index/about/about_us/privacy/human_rights.html
Last accessed 29th August 2011.

Wilcke, C., 2011. Jordan's Assault on Free Speech. *Human Rights Watch* [online]August 4th 2011. Available at:
http://www.hrw.org/news/2011/08/04/jordans-assault-free-speech
Last accessed 29th August 2011.

White, M., 2010. Clicktavism is ruining leftist activism. *The Guardian* 12th August [online]. Available at:
http://www.guardian.co.uk/commentisfree/2010/aug/12/clicktivism-ruining-leftist-activism
Last accessed 29th August 2011.

York, J., 2011. What Syria's unblocking of Facebook was really about. *Jillian York blog* [online] 6th May. Available at:
http://www.reuters.com/article/2007/11/23/us-syria-facebook-idUSOWE37285020071123
Last accessed 29th August 2011.

Zuckerman, E., 2010. Public Spaces, Private Infrastructure: Open Video Conference. *Ethan Zuckerman blog* [online]. Available at:
http://www.ethanzuckerman.com/blog/2010/10/01/public-spaces-private-infrastructure-open-video-conference/
Last accessed 29th August 2011.

Secondary Sources:

Castells, M., (2010) *The Rise of the Network Society: The Information Age: Economy, Society, and Culture.* Volume I, 2nd Edition, Wiley Blackwell, New Jersey.

Global Compact Network, 2010. *How To Do Business With Respect For Human Rights. A Guidance Tool For Companies*. Global Compact Network, Netherlands (Reprint sponsored by Shell).

Gunderson, J.L., 2006. *Multinational Corporations as Non State Actors in the Human Rights Arena* in 'Non-state actors in the human rights universe' pp 77-92 Andreopoulos Z.A. and Juviler P. (Eds.) Bloomfield, CT: Kumarian Press Inc.

Klein, N., 2002. *Fences and Windows. Dispatches From The Front Line Of The Globalisation Debate*. Flamingo, An imprint of Harper Collins publishing, Hammersmith, London.

Lauren, P.G., 1998. *The Evolution of International Human Rights: Visions Seen.* Philadelphia, University of Pennsylvania Press.

Lebert, J., 2002. *Information and Communication Technologies and Human Rights Advocacy: The Case of Amnesty International* in 'Civil Society in the Information Age' pp19-37 ed. Hajnal, P, Ashgate Publishing, England.

Morozov, E. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. Public Affairs, New York City.

Shell, 2002. Human Rights Dilemas. Available at: http://www-static.shell.com/static/environment_society/downloads/management_primers/human_rights_dilemmas.pdf
Last accessed 29th August 2011.

Van Rooy A., 2004, *The Global Legitimacy Game: Civil Society, Globalisation and Protest.* Palgrave Macmillan: Basingstoke.

Interviews:

Sameer Padania, Director of Macroscope and former Witness manager. Interviewed by Lucy Purdon at The British Library, Friday 12th August, 10.30am.

Appendix 1:

GLOSSARY

ATCA – Alien Tort Claims Act

BBM- BlackBerry Messenger

BT – British Telecom

CPJ – Committee for the Protection of Journalists

DDoS – Distributed Denial of Service

DEA – Digital Economy Act (UK)

EFF – Electronic Frontier Foundation

GC – Global Compact

GNI – Global Network Initiative

GP – Guiding Principle

HRC – Human Rights Council

HTTPS – Hypertext Transfer Protocol Secure

ICBL – International Campaign to Ban Landmines

ICCPR – International Covenant on Civil and Political Rights

ICESCR – International Covenant of Economic, Social and Cultural Rights

ICP – Internet Content Providers

ICT – Information and Communication Technology

ILO – International Labour Organisation

IOC – International Olympic Committee

IP – Intellectual Property

ISP – Internet Service Provider

MPA – Motion Picture Association

NGO – Non-governmental organisation

OECD – Organisation of Economic Cooperation and Development

PAYG – Pay As You Go

RAT – Remote Access Tool

RIM – Research in Motion (owner of BlackBerry)

SSL- Secure Socket Layer

TNC – Trans-national Corporation

UDHR – Universal Declaration of Human Rights

UN – United Nations

URL – Uniform Resource Locator