Global Network Initiative



Digital Freedoms in International Law

Practical Steps to Protect Human Rights Online

A report by Ian Brown & Douwe Korff

www.globalnetworkinitiative.org

About this Report

This report was commissioned by the Global Network Initiative (GNI) and was made possible by a grant from the Open Society Foundations. It is an academic work designed to pose questions and bring others into a dialogue. It attempts to tackle some of the most difficult questions around protecting rights to freedom of expression and privacy in the Information and Communications Technology (ICT) sector. We view this report as the beginning, rather than the end of a conversation, and we welcome feedback.

The report was written by Ian Brown and Douwe Korff and is based on extensive interviews with government, civil society and corporate actors involved in these matters, and draws on their practical experiences. We held three workshops, in London, Washington DC and New Delhi, with key stakeholders from all of these groups. Thanks to Eric King of Privacy International for providing the content for the Technology Exports to the Middle East map.

Please direct comments or questions to info@globalnetworkinitiative.org.

Dr. Ian Brown is Associate Director of Oxford University's Cyber Security Centre. He has led numerous EU and UK-funded research projects on privacy and information security, including a comparative study for the European Commission on the current revision of the Data Protection Directive, and co-authored with Douwe Korff a 2011 report on "Social Media and Human Rights" for the Council of Europe Commissioner for Human Rights. Dr Brown has consulted for the US Department of Homeland Security, JP Morgan, Credit Suisse, Allianz, McAfee, BT, the BBC, the Cabinet Office, Ofcom and the National Audit Office. He is a member of the UK Information Commissioner's Technology Reference Panel.

Professor Douwe Korff is a Dutch comparative and international lawyer. He is both a general human rights lawyer and a specialist in data protection. Following academic research at the European University Institute and at the Max Planck Institutes for comparative and international criminal- and public law, he taught at the University of Maastricht in the Netherlands and at the University of Essex in the UK. He is currently Professor of International Law at London Metropolitan University and visiting professor at the Universities of Zagreb and Rijeka in Croatia. He has carried out extensive work on data protection for the European Commission, the UK Information Commissioner, and industry, often with Ian Brown.

Disclaimer

The views expressed in this publication are those of its authors.

About GNI

GNI is a multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics, who have created a collaborative approach to protect and advance freedom of expression and privacy in the ICT sector. GNI provides resources for ICT companies to help them address difficult issues related to freedom of expression and privacy that they may face anywhere in the world. GNI has created a framework of principles and a confidential, collaborative approach to working through challenges of corporate responsibility in the ICT sector. Learn more at: http://www.globalnetworkinitiative.org

Table of contents

About this Report **2**

Executive summary **4**

1 Introduction **8**

1.1 Technologies of political activism and control 9
1.2 Protecting human rights and public safety online 11

2 International law standards **14**

2.1 Standards that apply in ordinary times 15
2.2 Standards that apply in times of war or national emergency 15
2.3 Standards that apply in relation to terrorism and other serious breaches of public order, falling short of war, internal armed conflict, or other national emergencies 18
2.4 Emerging standards on the actions of companies 22
2.4.1 The UN Guiding Principles on Business and Human Rights 22
2.4.2 The GNI Principles and Implementation Guidelines 26
2.5 Difficulties in applying the existing and emerging international standards in the digital environment 30

3 Export controls and licensing **33**

3.1 States' Responsibility to Protect 33
3.2 Dual use controls and the Wassenaar Arrangement 36
3.3 Protecting tools for activists 38
3.4 Transparency and non-Wassenaar producers 39
3.5 Technical standards 40
3.6 Civil liability and private rights of action 40

4 Recommendations **41**

4.1 Companies 41
4.2 Governments 43
4.3 Inter-Governmental Organisations 44
4.4 Non-Governmental Organisations 45
4.5 Investors 45

5 Endnotes **46**

Executive summary

With around 2.3 billion users, the Internet has become part of the daily lives of a significant percentage of the global population, including for political debate and activism. While states are responsible for protecting human rights online under international law, companies responsible for Internet infrastructure, products and services can play an important supporting role. Companies also have a legal and corporate social responsibility to support legitimate law enforcement agency actions to reduce online criminal activity such as fraud, child exploitation and terrorism. They sometimes face ethical and moral dilemmas when such actions may facilitate violations of human rights.

In this report we suggest practical measures that governments, corporations and other stakeholders can take to protect freedom of expression, privacy, and related rights in globally networked digital technologies. These are built on a detailed analysis of international law, three workshops in London, Washington DC and Delhi, and extensive interviews with government, civil society and corporate actors.

International law requirements

The International Covenant on Civil and Political Rights and related regional treaties protect online freedom of expression and privacy. States must ensure these protections for anyone within their effective power and control. In many instances they must also protect individuals against violations of their rights by other individuals or companies.

Restrictions on rights must be based on published, clear, specific legal rules; serve a legitimate aim in a democratic society; be "necessary" and "proportionate" to that aim; not involve discrimination; not confer excessive discretion on the relevant authorities; and be subject to effective safeguards and remedies.

In "time of war or other public emergency threatening the life of the nation", states can impose restrictions "to the extent strictly required by the exigencies of the situation", although not discriminate solely on racial or gender grounds. Emergency legislation should be passed in ordinary times when it can be fully debated and understood.

The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has recommended that anti-terrorism measures are overseen by the judiciary "so that they remain lawful, proportionate and effective, in order to ensure that the government is ultimately held responsible and accountable." This approach should be used with other breaches of public order that fall short of armed conflict.

Government agencies are increasingly asking Internet companies directly for customer data held outside their jurisdiction. When law enforcement or national security agencies in one country want to obtain access to evidence in another country, they generally have to go through "Mutual Legal Assistance Treaties" (MLATs) that protect the rights of all affected persons. MLATs are complex and can be cumbersome in practice. However, bypassing established MLAT processes constitutes an infringement of sovereignty.

Emerging company standards

The UN Guiding Principles on Business and Human Rights provide a comprehensive framework in which companies can address their responsibility to respect human rights. Companies faced with state demands that violate human rights have a duty to minimise the extent of any such cooperation. They must assess in advance the human rights risks in countries where they operate, take measures to minimise these risks, and help the victims of any enforced cooperation.

The GNI Principles also stress the need for companies to be pro-active in minimizing the impact of government restrictions on the rights to freedom of expression and privacy of their users; the need to build the principles into companies' basic policies, procedures and processes; and the need for due diligence and risk assessments.

Export controls and licensing

US and EU sanctions against repressive regimes such as Iran and Syria already include specific bans on the export of technologies and services that could aid in human rights violations. However, these will not prevent monitoring and censorship tools being acquired and built into the infrastructure of repressive regimes that are yet to reach this stage.

Many of these tools are "dual use", with legitimate network management and security purposes. Some are required for law enforcement purposes by democratic states. There are extensive international controls on the export of other "dual use" technologies with civil and military applications. However, many of the technologies we discuss can already be used to enable widespread repression, without that use being "military".

Technology companies have legitimate concerns that export controls limit access to potentially significant markets, and impose bureaucratic constraints on legitimate sales that may be ineffective against bad actors. A further danger is that controls block the provision of tools to democracy activists. This can happen through broad controls such as those applied by the US against Iran and Syria. But even when relaxed, the complexity of the controls and the harsh penalties for making a mistake still discourage many companies from allowing the use of their products by anyone in these countries.

Some software and telecommunications products require frequent updating by the vendor, or can be remotely disabled. Where such restrictions can be shown to be effective, the need for export controls on that equipment as a preventative measure is reduced, since usage controls can be put in place at any time.

Recommendations

On the basis of our analyses and building on the UN Guiding Principles and GNI Principles and Implementation Guidelines, we propose the following possible steps that can be taken to prevent or mitigate human rights violations perpetrated or facilitated by the use of globally networked digital technologies.

Companies

Companies should exchange information on legal systems and experiences in specific jurisdictions with other companies, governments and non-governmental organisations (NGOs). Before entering a market, companies should assess whether the domestic legal

systems and practices conform to international human rights and rule of law requirements. If authorities in the country are involved in human rights abuses, and if the technologies a company is considering selling there could contribute to such repression, it should carefully plan how it can make its technology available in a form that minimises the risk of abuse.

Companies should ensure they have a clear understanding of lawful procedures under which subscriber data can be requested, material blocked, and connections terminated. Where possible they should agree on specific points of contact for government requests, and mechanisms to check the authorisation of requests. Companies should share and collectively publish aggregate statistics about the use of these procedures, and challenge ambiguous demands in the higher courts.

Companies should use "Privacy by Design" principles to reduce the processing and storage of personal data no longer required for a legitimate business purpose, which could later be subject to compelled disclosure. In countries with deficient laws, this may include storing personal data outside the control of that jurisdiction. Companies' terms and conditions should specify that user data will only be provided to government agencies upon receipt of a legally binding request. Companies should insist that Mutual Legal Assistance (MLA) arrangements are the only appropriate means of cross-border data access.

If host country authorities demand *ad hoc* access to data in circumstances that suggest a potential violation of international human rights law, the company should challenge the demand before the courts of the host country, and resist attempts at access pending full judicial review of the demand. If the host country demands direct access to company data, through the insertion of opaque "black box" interception or access devices, the company should fundamentally consider its provision of the product to the country: such effectively unlimited and uncontrollable access is fundamentally contrary to basic principles of the rule of law, unless accompanied by a very strong control and oversight regime.

Governments

States should be willing to engage in dispute resolution measures to resolve conflicts over human rights compliance in the use of products sold and supported by companies from their country.

States should insist that demands for access to data held on their territory should be made only through the applicable Mutual Legal Assistance arrangements, and that extraterritorial demands for access to data on a server in their jurisdiction would otherwise constitute a violation of sovereignty. They should consider backing up such action in domestic law, and in inter-governmental arrangements and treaties. They should also consider applying civil legal liability to companies that fail to perform due diligence checks or to take measures to prevent, mitigate or end abuse of products for the perpetration of large-scale or serious human rights violations.

States should consider including tools that have primary or significant potential uses for human rights violations in "dual use" export control regimes, requiring suppliers to undertake extensive due diligence on end-users before export to or support, maintenance or training for specific repressive regimes. The maintenance of a list of controlled items and targeted states would require frequent multi-stakeholder discussion between states, technology companies, and human rights groups and academics with expertise in the use of these tools for human rights violations.

Tools useful for political activism should be more clearly excluded from export controls and sanctions. At a minimum, broad general licences, allowing the export of software and support as well as information, are easier to understand and comply with than a requirement for individual licensing procedures. Information security tool controls could be immediately scrapped.

Meaningful statistics and information should be published to allow the public to see how, how often, and in what kind of circumstances blocking technologies are used, and how personal data and communications of private citizens are being shared between Internet intermediaries and governments.

Inter-Governmental Organisations

Global and regional inter-governmental organisations (IGOs) should review MLA arrangements, to address the currently unresolved complex legal issues that arise under them. Such a review should also address the need to introduce speedy access to personal data under MLAs, subject to appropriate safeguards. Further research is needed into measures that can increase the responsiveness of MLA requests while protecting human rights and public policy objectives, and into conflict of laws issues that are currently arising.

IGOs should make clear that states may provide incentives to companies that act in accordance with these recommendations, and may impose disincentives on companies that act blatantly contrary to those recommendations. US and European calls for restrictions on Internet freedom of expression to be classified as barriers to trade should be given speedy consideration by the World Trade Organisation.

Non-Governmental Organisations

Human rights NGOs can play an important role in educating companies about relevant international standards, in training company staff on dealing with human rights concerns in countries in which they operate, and in the conduct of human rights impact assessments.

NGOs should support efforts to create stronger international law frameworks for the protection of human rights in relation to the sale and support of human rights sensitive products by companies. They should develop and campaign for stronger human rights law standards on how governments demand content removal /blocking and sharing of user data, given that specific governmental actions often have global implications.

NGOs should do more to raise public awareness about the roles and responsibilities of ICT companies in protecting people against human rights abuses, and how to make informed decisions as consumers and users when choosing between ICT products and services. They can also do more to educate people about how to protect themselves against human rights abuses when using ICTs in their daily lives as well as during political crises.

Investors

Socially responsible investors should expect companies to commit to appropriate human rights standards that meet three essential tests. Standards should have operational utility, addressing issues in a concrete, practical way. They should be developed and implemented in a multi-stakeholder process with NGOs, academic experts and other stakeholders. And they should require accountability through public reporting, even if certain details are held back in some extremely sensitive situations.

1 Introduction

With around 2.3 billion users, the Internet has become part of the daily lives of a significant percentage of the global population. In many countries this includes its use as an important platform for political debate and activism. Frank La Rue, the UN Special Rapporteur on freedom of expression, noted recently that it 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. Indeed, the recent wave of demonstrations in countries across the Middle East and North African region has shown the key role that the Internet can play in mobilizing the population to call for justice, equality, accountability and better respect for human rights."[1]

International law gives states the principal responsibility for protecting human rights. However, the broad ecosystem of companies responsible for Internet infrastructure, products and services can play an important supporting role.

Companies also have a legal and corporate social responsibility to support legitimate law enforcement agency actions to reduce online criminal activity such as fraud, child exploitation and terrorism. They sometimes face ethical and moral dilemmas when such actions may facilitate violations of their users' and other individuals' human rights.

In 2011, GNI commissioned a report that mapped the factors that can cause freedom of expression and privacy problems against the various sectors making up the global IT industry, such as service providers and hardware vendors.[2] The report concluded:

> *What is needed is a concerted effort, undertaken by the industry as a whole and its various stakeholders (including human rights groups, governments, investors, and academics) to explore how the human rights of freedom of expression and privacy can be most effectively protected in the context of legitimate law enforcement and national security activities.*

This report is a further step towards that concerted effort. It builds on the findings of the 2011 report, international human rights law, as well as on the broader work by other experts on business and human rights, to suggest practical measures that governments, corporations and NGOs can take to protect freedom of expression, privacy, and related rights in globally networked digital technologies.

We conducted extensive interviews with government, civil society and corporate actors involved in these matters, and draw on their practical experiences. We held three workshops, in London, Washington DC and New Delhi, with key stakeholders from all of these groups. We have included a number of their examples in the text.

Our analysis focuses on technologies that have the greatest impact on freedom of expression and privacy. We look at systems that can be used to block access to information at the nation-state level, in particular through blocking of Internet websites. Secondly, we examine technologies that can be used by states for mass surveillance of Internet activity and mobile phone use. In combination with data mining and "profiling" tools, these technologies can be used to identify and target minority groups and possible political opponents – which in repressive states exposes them to harassment, arrest, detention, torture and even death.[3]

The report is structured as follows:

- In the rest of this introduction we summarise the role that digital networked communications technologies now play in political activism, and the response of repressive regimes – as well as legitimate Internet-related state actions to protect public safety.
- In section 2 we outline the relevant international law standards, in relation to relatively normal times and times of national emergencies, as well as in relation to measures aimed at countering terrorism and major disturbances. We focus on the legal and practical difficulties of applying these standards in the new, global, public-private environment, as faced by companies, and how to overcome these difficulties.
- In section 3, we discuss arms control/export licence regimes, including in particular the Wassenaar Arrangement, to see whether technologies with serious potential for repression could be brought within these regimes, or equivalent measures be applied *mutatis mutandis*.
- In section 4 we summarise our recommendations for governments, companies, civil society groups, and investors.

1.1 Technologies of political activism and control

Over the last three years, the political ferment in Iran and many Arab countries has highlighted the role that digital networked communications technologies play in political activism and organisation, as well as the determined attempts this has provoked from repressive regimes to censor and monitor activists and block political change.

In Egypt, Libya, Yemen and Tunisia, campaigners coordinated and publicised mass protests using blogs, tweets, Facebook, online videos, and SMS messages – many of which were picked up by the global media and published around the world. These protests ultimately led to regime change, although the extent to which the Internet contributed to this is fiercely contested. But the governments of Syria, Bahrain and Iran have so far resisted change through a ferocious counter-response, including monitoring online communications to identify activists for arrest, torture and murder.

Repressive regimes are becoming increasingly adept at turning the online environment to their own advantage. The Iranian government, for example, asked the public for help in identifying individuals in photos of protests, published in online news media. Officials have checked the Facebook accounts of visiting Iranians at passport control, noting any suspicious-looking friends, and sent threatening messages and warnings to overseas Iranians that their relatives at home may be hurt if they support protests. Iranian ISPs have slowed and blocked access to sites criticising the regime. Voice and data communications have been widely monitored at centres originally installed by companies including Nokia Siemens Networks – using equipment built to meet demands from democratic governments for "lawful access" capabilities in their own communications networks.[4]

Iran is hardly alone in these activities. In a 2011 study, Freedom House identified fifteen countries that were engaging in "substantial blocking" of online political content. Twelve countries had imposed total bans on YouTube, Facebook, Twitter or equivalent services.

Technical attacks were used to disrupt activist networks, eavesdrop on communications, and cripple websites in a further twelve nations.[5]

These technologies and their repressive uses have been comprehensively documented.[6] Here, we would like to note a few matters in particular.

The first is that the scope and criteria for the use of surveillance and blocking technologies are not hard-wired into those technologies. It is difficult enough, even in democratic states with meaningful human rights protections, to ensure surveillance and blocking tools are used in an accountable and transparent way. Deep Packet Inspection hardware, for example, is used for network management, network security, building advertising profiles of users, as well as for the monitoring of communications. Real-time surveillance of high-bandwidth links within and between ISPs can require expensive equipment, but this is less of an issue for those small countries that are mainly interested in their relatively low volumes of international traffic. It is even difficult, in technical terms, to distinguish between surveillance of communications use data (such as who is talking to whom) and the contents of communications.[7]

Secondly, surveillance and blocking systems are highly portable, especially software components, and it is extremely difficult for states to control their export. However, the producers of these technologies frequently need to supply software updates. They are also often able to see if their technologies have been resold or exported, typically because of the use of new IP addresses in the communications between the producer and the user.

Finally, national-level filtering and “blocking” systems are at the same time relatively easy to by-pass, and tend to be seriously excessive in their application, by blocking access to many legitimate sites in addition to the few that were the intended targets.[8] This may not worry oppressive regimes, which may anyway be more interested in gathering data on individuals circumventing restrictions, but it makes the use of such technologies highly dubious in terms of international human rights law. The system configuration is again crucial.

The Internet and the Egyptian revolution

The Internet was one of the tools used in 2010-11 by Egyptians to organise protests against the regime of President Hosni Mubarak, and to expose electoral fraud and other government criminality. In turn Mubarak's regime monitored online activity and imprisoned, attacked and murdered journalists and activists, including 28-year old Khaled Mohammed Said, who had posted an online video about police corruption. A cybercafé owner reported that Said was arrested and beaten to death by two plainclothes policemen. A Facebook group called "We Are All Khaled Said" quickly gained nearly 100,000 members. The regime tried to slow and block online access to critical material and then the entire Internet as it was overwhelmed by protest in January 2011.

Local telecommunications companies, including Vodafone Egypt, were forced to comply with government orders to cut off phone and Internet connectivity for several days, and later to send pro-regime SMS messages to customers. These orders were given under Egypt's emergency laws, with a state of emergency having been continuously in place since 1981.

Companies have few options when given such orders, but their actions were heavily criticised. Egyptian blogger and activist Alaa Abd El-Fatah, in a speech to the Silicon Valley Human Rights conference, said that he did not expect companies to become revolutionaries – but he did want them to delay, protest, and demand court orders before complying.



The shutdown did not completely cut off Egyptians' Internet access. France Data Network and the Swedish activist group Telecomix both offered international dial-up accounts, while Google and Twitter set up a phone gateway allowing voice callers to leave audio recordings that were tweeted at @speak2tweet. Callers could also listen to previously recorded messages. Activists were able to provide continuing coverage of protests to outside media organisations such as the BBC World Service, which beamed them back into the country and all around the world.

1.2 Protecting human rights and public safety online

What can governments, technology companies and campaign groups do to reduce the recurrence of some of the shocking human rights violations recently seen in repressive regimes, whilst at the same time facilitating legitimate state action to protect public safety – especially in democracies under the rule of law? Much work has already been done to document government practices and address the roles of state and corporate actors.[9]

States have "positive" duties to protect the right to life and other crucial rights of individuals, such as against criminal and terrorist threats.[10] They have special duties in relation to the rights of the child.[11] As further discussed in section 2, states have the right, and in some cases the duty, to restrict some rights in order to protect others. In some special circumstances, they may impose further-reaching limitations.

The rights that we are most concerned with in this report – freedom of expression and information, privacy, and related rights such as freedom of communication and association – are all rights that can be limited in ordinary times, and even further limited in times of emergency, although always within certain legal parameters. The publication of certain types of information has been criminalised in almost every state. Images of child abuse are almost universally banned. Most European nations have criminalised the online distribution of "racist and xenophobic" material, threats and insults, and the denial or justification of "genocide or crimes against humanity".[12] Countries with a history of communal violence often ban material that could exacerbate such tensions.

In emergencies, most governments can shut down or restrict telecommunications networks. For example, after the 7 July 2005 London bombings, London police restricted mobile phone calls to pre-authorised emergency personnel for nearly five hours within a kilometre of a bombed train station.[13] These shutdowns can also obstruct attempts by individuals and companies to respond to an emergency, potentially leading to panic.

Providers of communications services are required by government agencies in almost every country to enable the lawful interception of communications and supply communications "meta-data" such as subscriber records, the sender and recipient of messages, and the location of users. These communications and data play an important role in counter-terrorism and criminal investigations, with the UK's Serious Organised Crime Agency reporting that "in 2006-7, lawful interception and communications data contributed to the recovery of £29m of criminal assets and stolen cash; 151 firearms being taken off the UK streets with the arrest of a number of gang members; some 830 arrests and the seizure of 3.5 tonnes of Class A drugs; and the rendering of assistance in 35 threat to life situations, leading to the prevention of a number of murders."[14] As a Nokia Siemens Networks representative told a European Parliament hearing after criticism of sales of mobile phone monitoring equipment to Iran:[15]

> *Today, governments in almost all nations require operators to deploy Lawful Interception as a condition of their license to operate. As a result, LI is present in almost every telecommunications network in the world, including those that are being used by probably everyone in this room today. And, for good reason: to support law enforcement in combating things like child pornography, drug trafficking and terrorism.*

Meeting all of these responsibilities can require a difficult balancing act. For corporate actors, GNI has issued Principles on Freedom of Expression and Privacy, and a set of Implementation Guidelines on these principles. It has also established a Governance, Accountability & Learning Framework to help companies and other stakeholders in the information and communications technology (ICT) industries to respect and protect freedom of expression and privacy globally through individual and collective actions. Regular independent assessments are carried out of companies' compliance with the principles and implementation guidelines.

Service providers play an important role in democracies in checking that warrants for interception and communications data are appropriately authorised, and in providing only the data that has lawfully been requested. One provider told us that they work with the most senior politicians to advocate warrants that are "publicly traceable, accountable and defined in law" – making clear that due process has been followed, that requests are proportionate, there is an appropriate degree of transparency, and that named individuals are clearly responsible. Another provider told us that the legitimacy or otherwise of requests for data is often clear given the user information available through their own systems, and suggested that providers need a "behind the scenes" mechanism to challenge the validity of requests when there are secrecy requirements attached.

Some governments have demanded that surveillance tools are directly inserted into communication systems, in the form of "black boxes" through which the authorities can directly access any data flowing through the system. This sometimes requires the cooperation of the communications providers concerned, although major intelligence agencies are adept at intercepting signals from undersea fibre optic cables, satellite downlinks, radio and microwave signals and other communications media.[16] A European telecommunications provider told us they were extremely reluctant to allow such opaquely functioning equipment to be attached to their network, although it may be a condition of market entry in some countries.

One of our interviewees pointed out that law enforcement officials will often have their actions questioned and judged in court, but that the same does not apply to the activities of national security agents. Judicial scrutiny is, in democratic states with independent courts, an important safeguard – although such scrutiny is still often limited when it comes to criminal intelligence activities, and limited to very specific oversight mechanisms in national security matters. In the UK, for instance, it is precisely because the police and intelligence agencies do not want to expose their surveillance techniques that the results of communications intercepts are not admissible in court.

Historically, telecommunication systems were tied to a particular country, and often originally state-owned and run. Most of the data processed in such systems still tends to be kept on servers of those companies, situated in the country in question. However, companies increasingly store and process customer data in remote data centres ("the cloud"). For the moment at least, these companies and data centres are mainly based in democracies that respect the rule of law. This has implications in relation to demands for access to the data, made by government agencies in the country where companies and data centres are based and used. India and Saudi Arabia have both demanded that companies hold data from their own residents on local servers, where they can more easily be accessed by law enforcement and national security agencies.

2 International law standards

The use of the technologies we described in section 1 affect a range of fundamental rights: freedom of communication, freedom of association, freedom to seek, receive and impart information and ideas without interference by public authorities, regardless of frontiers and through any medium, freedom of information, and freedom from surveillance and intrusion into one's private life and social and political activities. They can also impact on the economic, social and cultural rights of individuals and groups, especially cultural, religious, ethnic or national minorities, and women.

All these rights are recognised in the main international human rights instruments, such as the Universal Declaration of Human Rights and the International Covenants on Civil and Political Rights (ICCPR) and on Economic, Social and Cultural Rights (which together constitute the UN Bill of Rights), and in regional instruments including the European Convention on Human Rights (ECHR) and the Council of Europe's Social Charter, the American Convention on Human Rights, and to a somewhat lesser extent in the African Charter on Human and peoples' Rights.

Below, we will focus on the rights to freedom of expression and privacy. However, even with this limitation, the application of these standards is not simple.

Current international human rights law essentially applies to states, and actions and omissions of public bodies only. Different standards apply in normal times, and in times of war or national emergency. The exceptions that can be invoked in times of serious political upheaval falling short of such emergencies, and in relation to anti-terrorist measures, is decided in light of the circumstances.

Secondly, there are special problems in applying law generally, and human rights law in particular, to the new global, digital environment. Laws are still mainly drawn up for an environment with clearly defined territorial jurisdictions. And much of the control over the Internet rests in the hands of private companies, whereas traditional human rights law almost entirely focussed on states. This raises problems of both "prescriptive" and "enforcement" jurisdiction, and of "privatised" (or semi-privatised) law enforcement, without adequate remedies.

Third, there is the fact that in law and in practice some countries are worse than others. Some countries have laws that are generally compatible with international human rights standards and generally good practices, independent courts and fair and effective remedies. Others either have serious deficiencies in their laws as far as global human rights standards are concerned, or fail to comply with them in practice, or have courts and remedial systems that are not free and independent. The worst show all of these failings.

Finally, the "horizontal" application of these already complex standards to acts and omissions of companies is only indirect and limited, although new standards are emerging that deal more directly with them. These include the Guiding Principles on Business and Human Rights, drafted by the Special Representative of the UN Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie (the "Ruggie Principles") and, of course, the GNI Principles on which we build.

In this section, we set out the accepted international human rights standards that should be adhered to by all states, and the more tentative standards to be complied with by

companies. Of course, many governments fail to live up to their duties, and many companies do not yet subscribe to good governance and human rights-friendly rules. But it is the purpose of this report to help bring practice more in line with these norms, and we hope our recommendations will contribute to that.

2.1 Standards that apply in ordinary times

In normal times, any restrictions on the rights to freedom of expression and information, privacy and other rights such as the rights to freedom of communication and association must meet certain standards. Under the International Covenant on Civil and Political Rights and regional human rights treaties, these restrictions must:[17]

1. Be based on "law" – on published, clear and specific legal rules, the application of which is reasonably foreseeable;
2. Serve a legitimate aim in a democratic society. This of course includes law enforcement and the protection of national security. However, limitations imposed for such reasons should not be abused for other ends, such as to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest (Johannesburg Principles Principle 2b);
3. Be "necessary" and "proportionate" to that aim, and not impair the essence of the right;
4. Not involve discrimination based on race, colour, sex, language, religion, political or other opinion, national or social origin, nationality, property, birth or other status;
5. Not confer excessive discretion on the relevant authorities; and
6. Be subject to effective (judicial) safeguards and remedies.[18]

States must ensure the above limits on restrictions of rights not just in respect of their own citizens, but also for anyone else who is within their territory or jurisdiction, or even, as regards extra-territorial acts, within their effective power and control.[19]

States must, moreover, in many of the instances relevant to our report, protect individuals against violations of their rights not just by their own public authorities, but also, where relevant and appropriate, against actions by other individuals, or other private entities such as companies, that result in undue restrictions or interferences with their rights (so-called "indirect" or "horizontal" effect of human rights provisions).[20]

2.2 Standards that apply in times of war or national emergency

In certain extreme circumstances, states can impose restrictions on many of the rights and freedoms guaranteed in the international human rights treaties, that go beyond the "normal" restrictions described above: they can "derogate" (partially deviate) from their obligations in respect of these rights. These "derogable" rights include all the ones most relevant to our study: freedom of expression, freedom of communication, freedom of association, freedom of information and privacy.[21]

Derogations of this kind are allowed only “In time of war or other public emergency threatening the life of the nation”.[22] However, the derogation provisions in the human rights treaties do not give states *carte blanche* to disregard the “derogable” rights as they please - far from it.

Thus, first of all, states may only adopt measures derogating from their normal obligations “to the extent strictly required by the exigencies of the situation” (Art. 4(1) ICCPR, Art. 15(1) ECHR).

Secondly, the ICCPR stipulates that the measures may “not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin” (Art. 4(1)). Other UN documents make clear that this applies in particular to the use of “profiles” in the fight against terrorism, but it is clear - and also follows from the status of the principle of non-discrimination as a rule of *jus cogens*, that is, as a most serious binding (peremptory) rule in international law - that this also applies in emergencies threatening the life of the nation.[23]

And third, the ICCPR in particular adds the important procedural safeguard that the existence of any such emergency must be “officially proclaimed” (Art. 4(1)). Moreover, states that do proclaim such an emergency and derogate from provisions in the ICCPR must immediately inform the other state parties to the Covenant of the provisions from which it has derogated and of the reasons for the derogations (Art. 4(3)).

The Human Rights Committee (which is the supervisory body overseeing implementation of the ICCPR and which issues guidance on its interpretation and application) has addressed the question of derogations twice, in 1981 and 2001, in two “General Comments”.[24] The UN standards are also usefully summarised in a UN document, Fact Sheet No. 32, to which we will return in more detail below.[25]

The international human rights standards applicable in times of emergency have also been addressed in the so-called Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, the Paris Minimum Standards of Human Rights Norms in a State of Emergency and the Johannesburg Principles on National Security, Freedom of Expression and Access to Information.[26]

Here, it must suffice to briefly highlight the main requirements of relevance to companies faced with demands made upon them under emergency laws that may impact on the fundamental rights and freedoms of individuals, including their customers (and to embassies that should support them, as discussed in section 4.2).

States must put emergency legislation on their statute book in ordinary times (rather than rush through special laws once an emergency has arisen), so that everyone who might be affected by such legislation - including companies - can know what might happen in special circumstances.

These laws must meet the normal “quality requirements” of “law”, i.e., they must be published as well as clear, specific and foreseeable in their application; and they must not grant excessive discretion to the authorities implementing the emergency provisions. They must preserve the powers of the courts to review the compatibility of both the provisions of these laws with the relevant constitutional and international law requirements, and the manner in which those provisions are applied. Courts should not defer to the assessments of political bodies (like the government, or certain ministers) as to whether there is an emergency, and as to what is necessary to meet the emergency.

Such laws may only be brought into force in serious emergencies that pose an actual or manifestly imminent threat to the physical integrity of the population, the political independence or the territorial integrity of the state or the existence or basic functioning of institutions indispensable to ensure and protect the rights recognized in the Covenant (and the question of whether this is the case should be fully justiciable).

Any emergency in which such laws are brought into force must be officially proclaimed. That proclamation, or information published immediately after it (to the general public, domestic and international), must clearly specify:

- The provisions of the international human rights instruments and the Constitution from which the state has derogated;
- A copy of the proclamation of the emergency, together with the constitutional provisions, legislation, or decrees governing the state of emergency (so as to allow for an assessment of the scope and constitutional and international law validity of the derogation);
- The effective date of the imposition of the state of emergency and the period for which it has been proclaimed;
- An explanation of the reasons which actuated the government's decision to declare an emergency and to derogate from its normal obligations, including a description of the factual circumstances leading up to the proclamation of the state of emergency; and
- A description of the anticipated effect of the derogation measures on the rights recognized by relevant international human rights instruments and the constitution, including copies of decrees derogating from these rights issued prior to the notification.

If a particular threat to public order or national security can be met by the normal laws, under the normal limitation clauses relating to the relevant human rights, then that is how that threat should be met. In such cases, recourse to emergency laws going beyond the ordinary limitations are not justified and contrary to international law.

When restrictions are placed on fundamental rights that exceed the normal restrictions, those restrictions should still be necessary and proportionate to those circumstances, not just in general or in the abstract, but specifically also in relation to individual cases. The question of whether they meet that standard, in each case, should remain fully justiciable.

If any emergency measures are applied in a way that either specifically targets, or has specific negative effects in relation to, certain individuals or groups because of their race, colour, ethnicity, language, gender, religion or social origin - then irrespective of whether this is intended, it constitutes a form of discrimination that violates international law and remains illegal under international law even in times of emergency.

The references above to the courts being able to adjudicate on matters such as the existence of an emergency, or the need for derogations from the normal rules (including the normal limitations on fundamental rights, in ordinary times), shall be read as including the possibility for individuals and others affected by the emergency laws or rules to refer both the general questions, and the application of the special rules in their specific cases, to the courts for free and impartial adjudication. All individuals and groups - and companies -

affected by emergency laws and rules and practices must have an effective remedy to challenge such laws, rules and practices in court, and the courts must be under a duty to deal with such challenges *ad fundum*, i.e., not merely by assessing whether the relevant formalities have been complied with.

We believe that the above provides for a basis for effective actions by companies and democratic governments supporting companies, as further discussed in section 4.

2.3 Standards that apply in relation to terrorism and other serious breaches of public order, falling short of war, internal armed conflict, or other national emergencies

Terrorism is abhorrent and a threat to society. As the UN Fact Sheet No. 32 puts it:

> *"Terrorism clearly has a very real and direct impact on human rights, with devastating consequences for the enjoyment of the right to life, liberty and physical integrity of victims. In addition to these individual costs, terrorism can destabilize Governments, undermine civil society, jeopardize peace and security, and threaten social and economic development. All of these also have a real impact on the enjoyment of human rights.*
>
> *Security of the individual is a basic human right and the protection of individuals is, accordingly, a fundamental obligation of Government. States therefore have an obligation to ensure the human rights of their nationals and others by taking positive measures to protect them against the threat of terrorist acts and bringing the perpetrators of such acts to justice." (p. 1)*

However, the adoption of undue measures to counter terrorism can also pose a serious threat to democracy, human rights and the rule of law. The UN and regional intergovernmental or supranational organisations such as the Council of Europe and the European Union have long engaged with these difficult issues and the dilemmas they pose, albeit without having fully resolved them.[27] Here, it must suffice to note the main thrust of the international approaches in this respect, with reference mainly to the "Ten areas of best practices in countering terrorism", identified in the latest annual report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin,[28] the UN Factsheet on Human Rights, Terrorism and Counter-Terrorism,[29] the Council of Europe Guidelines on Human Rights and the fight against terrorism,[30] and the Johannesburg Principles.[31]

These documents firstly state that effective counter-terrorism measures and the protection of human rights are not conflicting goals, but complementary and mutually reinforcing ones. They go on to stress that while sometimes acts of terrorism, or a terrorist campaign, may bring about an "emergency threatening the life of the nation", or may amount to a (usually non-international) armed conflict, there is a serious risk in assuming this too readily, and to resort too quickly to measures that contravene the normal human rights standards discussed above, i.e. to unduly invoke the derogations. This is aggravated by the fact that anti-terrorist or counter-insurgency measures have a tendency to become semi-permanent. They also often include transferring powers to military authorities.

Another danger is that in domestic law the concept of "terrorism", and thus the scope of anti-terrorist measures, is stretched to include relatively minor acts and offences, especially when related to political, social or trade union activities.[32]

In these respects, the Special Rapporteur recommends as his third "best practice":[33]

> *To the broadest possible extent, measures against terrorism shall be taken by the civilian authorities entrusted with the functions related to the combating of crime, and in the exercise of their ordinary powers.*
>
> *Unless a state of emergency has been officially declared because terrorism genuinely threatens the life of the nation and requires the adoption of measures that cannot be undertaken through restrictions already permitted under international human rights law, terrorism does not trigger emergency powers.*
>
> *Where the law includes particular provisions that, for a compelling reason, are considered necessary in combating terrorism and entrust certain authorities with specific powers for that reason, the use of such powers for any purpose other than the combating of terrorism, as properly defined pursuant to practice 7, is prohibited.*

In line with this, the Special Rapporteur proposes a definition which limits the concept of terrorism - and thus the legitimate scope of anti-terrorist laws and measures - to hostage-taking, killings or serious physical violence undertaken for the purpose of provoking a state of terror or of compelling a government or international organization to do or abstain from doing something.[34] Note that this excludes doing "damage to property" for such a purpose, which is included in the contentious definition of terrorism in the Draft UN Comprehensive Convention on International Terrorism,[35] and which can much too easily be applied to large-scale demonstrations, blocking of ports or highways, etc., in the context of political or trade-union protests.[36] As the UN Fact Sheet puts it:[37]

> *clear safeguards must exist to ensure that [derogations and limitations in human rights treaties] are not used to curb the rights of political opposition parties, trade unions or human rights defenders.*

The Special Rapporteur also proposes (on the basis of Article 5 of the COE Convention on the Prevention of Terrorism), that acts should only be regarded as (and only be prosecutable as) "incitement to terrorism", if they fall within the following description of that crime:[38]

> *It is an offence to intentionally and unlawfully distribute or otherwise make available a message to the public with the intent to incite the commission of a terrorist offence, where such conduct, whether or not expressly advocating terrorist offences, causes a danger that one or more such offences may be committed.*
>
> (Practice 8. Model offence of incitement to terrorism)

The Johannesburg Principles also expressly limit legitimate restrictions on freedom of expression on grounds of national security to situations in which a government can demonstrate that: (a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence (Principle 6). They usefully expand on the kinds of expressions that should never be regarded as a threat to national security (or, we may add, be brought within the scope of anti-terrorist or wider emergency legislation):

Principle 7: Protected Expression

(a) Subject to Principles 15 and 16 [concerning release of official information], the peaceful exercise of the right to freedom of expression shall not be considered a threat to national security or subjected to any restrictions or penalties. Expression which shall not constitute a threat to national security includes, but is not limited to, expression that:

(i) Advocates non-violent change of government policy or the government itself;

(ii) Constitutes criticism of, or insult to, the nation, the state or its symbols, the government, its agencies, or public officials, or a foreign nation, state or its symbols, government, agencies or public officials;

(iii) Constitutes objection, or advocacy of objection, on grounds of religion, conscience or belief, to military conscription or service, a particular conflict, or the threat or use of force to settle international disputes;

(iv) Is directed at communicating information about alleged violations of international human rights standards or international humanitarian law.

(b) No one may be punished for criticizing or insulting the nation, the state or its symbols, the government, its agencies, or public officials, or a foreign nation, state or its symbols, government, agency or public official unless the criticism or insult was intended and likely to incite imminent violence.

The UN Special Rapporteur adds that individuals and entities (organisations) should only be listed as "terrorists" or "terrorist organisations" when there are "*reasonable grounds to believe that the individual or entity has knowingly carried out, participated in or facilitated a terrorist act (as properly defined pursuant to practice 7 above)*".[39]

We would add that individuals should not be treated as terrorists merely on the basis of some links with, or some expressions of support for, organisations that have been involved in (some) acts of violence, or some of whose members may have been involved in such acts. We know from experience that it is precisely this "bringing forward" of the criminal law, and especially of anti-terrorist laws, that poses a grave threat to human rights and freedom of expression.[40]

And finally, in terms of substantive law, we should note that the principle of non-discrimination also applies to anti-terrorist measures. Indeed, it has some special importance in this context, in particular in relation to "profiling" as a means of trying to identify actual or potential terrorists. A range of high-level human rights bodies and experts has expressed grave concerns about the serious risk of discrimination that profiling poses in this context, and has urged tight controls and judicial supervision.[41]

In addition, there is the always-crucial matter of the need for appropriate remedies. We have already noted that even in times of emergencies threatening the life of a nation, crucial issues must remain fully justiciable. The same applies *a fortiori* to anti-terrorist

measures. As it was put in a report by independent UN expert Robert K. Goldman, with reference to the debates and studies from the 1970s onwards:[42]

> *Many of these studies found that human rights were often at heightened risk of abuse, even in democracies, where emergency powers were increasingly concentrated in the executive branch. In order to prevent such abuses, these reports stressed the need for states to guarantee the independence and supervisory powers of the civilian judiciary during all emergency situations.*
>
> *This admonition is no less relevant in today's struggle against terrorism than it was some 20 years ago...* (paras. 13 – 14)

Consequently, it was "*a recurring theme in this report ... that civilian courts must have jurisdiction to review the provisions and supervise the application of all counter-terrorist measures without any pressure or interference, particularly from the other branches of government.*" (para. 15, emphasis added)

The above is re-affirmed in UN Fact Sheet No. 32 with specific reference to freedom of association,[43] and in the COE Guidelines on Human Rights and the Fight against Terrorism in relation to measures that interfere with privacy:[44]

> *Measures used in the fight against terrorism that interfere with privacy (in particular body searches, house searches, bugging, telephone tapping, surveillance of correspondence and use of undercover agents) must be provided for by law. It must be possible to challenge the lawfulness of these measures before a court.*

More important yet, the principle is affirmed more generally and forcefully by the UN Special Rapporteur on Human Rights and Terrorism, Martin Scheinin, in his 2006 report to the UN. Quoting the Goldman paragraph highlighted above, he writes:[45]

> *This principle is fundamental in the context of counter-terrorism, where governments can hide behind the banner of classified information to limit the rights of freedom of assembly or peaceful association based on confidential information which can neither be verified nor contested. The Special Rapporteur stresses that any decisions which limit human rights must be overseen by the judiciary, so that they remain lawful, proportionate and effective, in order to ensure that the government is ultimately held responsible and accountable.* (para. 29)

Essentially, other breaches of public order, falling short of war, internal armed conflict, or other national emergencies, should be dealt with in the same way. It should not be too readily assumed that such other emergencies warrant derogations from the normal human rights standards - in principle, they should be dealt with under the normal rules on limitations of rights. The measures adopted in this regard should be strictly limited in scope (including geographical scope) and time, and fully subject to judicial review, both in terms of whether the relevant formal and procedural requirements are met, and as to whether the actual measures taken meet the international standards of "law", "legitimate purpose", "necessity" and "proportionality".

Between them, the detailed substantive and procedural requirements of international human rights law, set out above, provide a sound basis for companies trying to implement the GNI Principles to make the relevant assessments as to whether demands from governments made to them, under either ordinary law or emergency- or anti-terrorist law,

meets the relevant international requirements. Obviously, however, the actual assessments in individual cases or specific country circumstances will not be easy. We therefore use them as the bases for our recommendations, set out in section 4.

Before proceeding to those, however, we must first address one further crucial issue: the question of whether, and if so when and how, these standards apply to the actions of companies. We also need to note the special problems that arise in applying the standards in the special contexts we are discussing. We will deal with those questions next, in sections 2.4 and 2.5.

2.4 Emerging standards on the actions of companies

International human rights law essentially applies only to states, and to actions (or omissions) of public authorities. Sometimes, it can be given what is somewhat mistakenly referred to as "horizontal effect", in that it is applied, indirectly, in relation to actions (or omissions) of private actors. But even then, the relevant obligations still rest on the state. The state is, in such cases, held responsible for the fact that it did not control the actions of the relevant private actors that impinged on human rights of individuals. Individual victims cannot invoke international law rules against private parties.[46]

This is problematic in the context of the issues we address, and more specifically in relation to the use of the Internet and mobile technology. The relevant technologies are mainly managed by private-sector entities, and the human rights violations we are trying to address have their origin in demands by governments that those private-sector entities cooperate with them in law enforcement, national security or anti-terrorist measures (or at least measures claimed to be for those purposes).

It is therefore important to note that new international standards are emerging, intended to be applied by companies. The most important are the UN Guiding Principles on Business and Human Rights (the "Ruggie Principles").[47] The GNI Principles and Implementation Guidelines, elaborated by GNI several years earlier, fit into and significantly extend the Ruggie framework. The European Commission has also recently begun a dialogue regarding the implementation of the Guiding Principles in the Information and Communication Technology sector.[48]

2.4.1 The UN Guiding Principles on Business and Human Rights

The UN Guiding Principles on Business and Human Rights provide a comprehensive framework in which companies can address their responsibility to respect human rights. The Special Representative summarised this framework in an earlier report as:[49]

> *[A] conceptual and policy framework to anchor the business and human rights debate, and to help guide all relevant actors. The framework comprises three core principles: the state duty to protect against human rights abuses by third parties, including business; the corporate responsibility to respect human rights; and the need for more effective access to remedies. The three principles form a complementary whole in that each supports the others in achieving sustainable progress.*

As noted below, the Ruggie Principles are useful in many respects, and we draw on them to develop our own recommendations. However, they tend to focus on possible human rights violations by companies and the duty of "host" states to take measures against such

violations.[50] They do not deal in detail with the converse situation, in which states that perpetrate serious human rights violations make demands of companies that, if acceded to, would lead to violations of international human rights law, and involve those companies in them.

However, the Special Rapporteur does stipulate that:[51]

> *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. And it exists over and above compliance with national laws and regulations protecting human rights.*

In other words, in principle, companies faced with state demands and laws that violate human rights have a duty to refuse to do so where they can, and minimise the extent of any such cooperation to the least possible in the circumstances.

This brings in a second point made by the Special Representative:[52]

> *Addressing adverse human rights impacts requires taking adequate measures for their prevention, mitigation and, where appropriate, remediation.*

That is to say: companies should think in advance of possible risks arising from undue state demands made upon them, and they should take measures – including technical measures – to try and make it possible for them to deny or at least minimise their cooperation. They must afterwards help the victims of their enforced cooperation with such allegedly undue and illegal state actions, to alleviate the harm done as much as possible. The latter should in our opinion at least include informing those victims of unlawful actions taken by the state, and of any enforced cooperation they had to provide.

Indeed, in the two paragraphs in which Ruggie does specifically deal with the danger of complicity of companies in human rights violations by state entities, he stresses that there may be serious legal consequences for this:[53]

> *Some operating environments, such as conflict-affected areas, may increase the risks of enterprises being complicit in gross human rights abuses committed by other actors (security forces, for example). Business enterprises should treat this risk as a legal compliance issue, given the expanding web of potential corporate legal liability arising from extraterritorial civil claims, and from the incorporation of the provisions of the Rome Statute of the International Criminal Court in jurisdictions that provide for corporate criminal responsibility. In addition, corporate directors, officers and employees may be subject to individual liability for acts that amount to gross human rights abuses.*
>
> *In complex contexts such as these, business enterprises should ensure that they do not exacerbate the situation. In assessing how best to respond, they will often be well advised to draw on not only expertise and cross-functional consultation within the enterprise, but also to consult externally with credible, independent experts, including from governments, civil society, national human rights institutions and relevant multi-stakeholder initiatives.*

As the GNI Principles reflect and operationalise, companies' responsibilities go beyond merely trying to avoid exacerbating the situation, and extend to a duty to take preventive

action to try and avoid such complicity, contemporaneous action to mitigate it where unavoidable, and remedial action where it occurred. In our opinion, this fits in with the Special Representative's other proposals, discussed below.

Thus, crucially, the Ruggie Principles provide for a corporate framework of "operational principles"[54] that include a requirement that companies adopt a company human rights policy, adopted and supported at the highest level, and embedded in all the company's overall operational policies; and crucially, for human rights due diligence. The latter is described as follows:[55]

> *In order to identify, prevent, mitigate and account for how they address their adverse human rights impacts, business enterprises should carry out human rights due diligence. The process should include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed. Human rights due diligence:*
>
> *(a) Should cover adverse human rights impacts that the business enterprise may cause or contribute to through its own activities, or which may be directly linked to its operations, products or services by its business relationships;*
>
> *(b) Will vary in complexity with the size of the business enterprise, the risk of severe human rights impacts, and the nature and context of its operations;*
>
> *(c) Should be ongoing, recognizing that the human rights risks may change over time as the business enterprise's operations and operating context evolve.*

Ruggie usefully stresses that human rights due diligence must go "*beyond simply identifying and managing material risks to the company itself, to include risks to rights-holders*" (i.e., to individuals whose human rights may be at risk); and that it "*should be initiated as early as possible in the development of a new activity or [business] relationship*".[56]

However, again, Ruggie's human rights due diligence principle does not seem to cover adverse human rights impacts that the business enterprise may cause or contribute to (or become complicit in), if it accedes to state demands that violate international human rights standards. Even so, the GNI Principles emphasise that human rights due diligence on the part of companies should also cover such possible situations.

The same therefore applies to the requirement repeated here by the Special Representative (with reference also to Principle 22), that:[57]

> *Human rights risks are understood to be the business enterprise's potential adverse human rights impacts. Potential impacts should be addressed through prevention or mitigation, while actual impacts – those that have already occurred – should be a subject for remediation.*

More specifically, the Special Representative refers, in several instances, to the possibility of a company becoming complicit in human rights violations by other entities – but those principles appear to be dealing only with situations in which those "other entities" are other companies, and in particular other companies with which the company has *business relationships*. A core premise of GNI is that these principles can and should be applied

mutatis mutandis to situations in which companies may be implicated in human rights violations by states. Ruggie suggests the following:[58]

> *Where a business enterprise contributes or may contribute to an adverse human rights impact, it should take the necessary steps to cease or prevent its contribution and use its leverage to mitigate any remaining impact to the greatest extent possible. Leverage is considered to exist where the enterprise has the ability to effect change in the wrongful practices of an entity that causes a harm...*
>
> *There are situations in which the enterprise lacks the leverage to prevent or mitigate adverse impacts and is unable to increase its leverage. Here, the enterprise should consider ending the relationship, taking into account credible assessments of potential adverse human rights impacts of doing so.*
>
> *Where the relationship is "crucial" to the enterprise, ending it raises further challenges. A relationship could be deemed as crucial if it provides a product or service that is essential to the enterprise's business, and for which no reasonable alternative source exists. Here the severity of the adverse human rights impact must also be considered: the more severe the abuse, the more quickly the enterprise will need to see change before it takes a decision on whether it should end the relationship. In any case, for as long as the abuse continues and the enterprise remains in the relationship, it should be able to demonstrate its own ongoing efforts to mitigate the impact and be prepared to accept any consequences – reputational, financial or legal – of the continuing connection.*

GNI suggests that this should apply not just to a company's business relationships with other companies, but equally to its relationships with the host state. Companies may often lack leverage over that state - but if state abuses are serious and continue in spite of protests and other action aimed at mitigating them (at least to the extent that the company is implicated in them), the company must be prepared to accept the consequences in terms of reputation, financial costs and legal challenges, or end the relationship, i.e. cease its operations in the country.

Moreover, the GNI states that the leverage referred to here should not be limited to a simple assessment of whether the company could force the state to end its human rights violations (or even merely those that it is forced to be complicit in). Rather, companies can also work with their home governments to exert pressure on the states violating human rights; and they should try and initiate such cooperation with their own governments or embassies wherever possible. And governments of democratic states should use their influence to support companies facing unlawful demands from repressive states, if needs be to the extent of directly interfering in the companies' businesses, e.g., through export control arrangements. We will return to these matters in our recommendations.

Equally important is the question of recording the companies' actions, and reporting on them. As Ruggie puts it:[59]

> *In order to account for how they address their human rights impacts, business enterprises should be prepared to communicate this externally, particularly when concerns are raised by or on behalf of affected stakeholders. Business enterprises whose operations or operating contexts pose risks of severe human rights impacts*

should report formally on how they address them. In all instances, communications should:

(a) Be of a form and frequency that reflect an enterprise's human rights impacts and that are accessible to its intended audiences;

(b) Provide information that is sufficient to evaluate the adequacy of an enterprise's response to the particular human rights impact involved;

(c) In turn not pose risks to affected stakeholders, personnel or to legitimate requirements of commercial confidentiality.

Although the above can take various forms, Ruggie adds, "*[f]ormal reporting by enterprises is expected where risks of severe human rights impacts exist, whether this is due to the nature of the business operations or operating contexts.*" [60]

Finally, Ruggie addresses the question of remedial action if a company has become involved in human rights violations, either directly, or through its business partners. His recommendations in this respect again focus on how host states and their institutions should be able to provide for remedies for victims to seek redress against the company. These are of little relevance in circumstances in which it is the host state itself that is the perpetrator of the violations, and that compelled the company to become complicit in those. GNI is working actively to develop an engagement and grievance mechanism broadly in line with that suggested by Ruggie.

However, as we noted earlier, Ruggie points out that in some circumstances companies can become legally liable for human rights violations by states that they helped to perpetrate. In extreme cases, this can include international criminal liability. In the kinds of cases that we are talking about, it is more likely to consist of civil liability for the companies' actions, in particular in their home state if that is one in which human rights are given strong protection.

In our opinion, practice consistent with the Ruggie principles we have outlined, including those we applied *mutatis mutandis* to situations in which companies are forced to become complicit in violations of human rights by host states, can and should have a significant impact on the question of liability. If a company acted in accordance with the principles, and thus took all possible measures to avoid being enrolled in a state's repressive actions, minimised any unavoidable involvement, and revealed its involvement-under-duress and helped possible victims - then the company could reduce its liability, and certainly avoid punitive damages.

By contrast, if a company negligently failed to perform human rights due diligence - if it took no measures to avoid being used, or to minimise its involvement, or if it kept its involvement secret and failed to help the victims - then that should impact on any civil liability it may have in its home state (or indeed elsewhere).

Indeed, states that want to provide strong support for human rights protection could legislate to impose such liability, and we include this in our recommendations.

2.4.2 The GNI Principles and Implementation Guidelines

The GNI was established, four years before the Ruggie Principles were published, specifically to address the fact that ICT companies, including Internet Service Providers, telecommunications companies and other service providers such as social networking sites,

increasingly face pressure by governments to act in ways that may impact the fundamental human rights of privacy and freedom of expression of their users. GNI provides a framework of principles ("the GNI Principles") and supporting guidance ("Implementation Guidelines") to such companies, as well as a "Governance, Accountability and Learning Framework". Companies that participate in the Initiative and sign up to the Principles accept that they have specific duties to respect and protect these rights.[61]

Here, it will suffice to note that the Principles, Guidelines and Framework fit in well with the Ruggie Principles – and fill many of the gaps discussed in the previous section. Like the Ruggie Principles, the GNI Principles stress the need for companies to be pro-active in trying to avoid or minimize the impact of government restrictions on the rights to freedom of expression and privacy of their users;[62] the need to build the principles into companies' basic policies, procedures and processes; and the need for due diligence and risk assessments, in cooperation with other stakeholders.[63] The latter should include "consideration of relevant local laws in each market and whether the domestic legal systems [and we may add, practices] conform to rule of law requirements". Unlike the Ruggie Principles, which do little to address a key problem faced by Internet intermediaries that governments can be the driver of human rights violations, the GNI focuses specifically on that problem.

Importantly, the Implementation Guidelines spell out certain standards that companies should adopt when faced with government demands that impact on the rights to freedom of expression and/or privacy of their users.[64] Companies faced with demands from governments which, if acceded to, might violate their users' or consumers' human rights, should:

- Require that governments follow established domestic legal processes when they are seeking to restrict freedom of expression/are seeking access to personal information;
- Interpret government restrictions and demands so as to minimize the negative effect on freedom of expression/narrowly interpret the governmental authority's jurisdiction to access personal information, such as limiting compliance to users within that country.
- Interpret the governmental authority's jurisdiction so as to minimize the negative effect on freedom of expression/narrowly Interpret and implement government demands that compromise privacy;
- Seek clarification or modification from authorized officials when government restrictions [or demands] appear overbroad, [unlawful], not required by domestic/applicable law or inconsistent with international human rights laws and standards on freedom of expression/privacy.
- Request clear written communications/[clear communications, preferably in writing] from the government that explain the legal basis for government restrictions to freedom of expression/demands for personal information, including the name of the requesting government entity and the name, title and signature of the authorized official.
- Challenge the government in domestic courts or seek the assistance of relevant [government] authorities, international human rights bodies or non-governmental

organizations when faced with a government restriction/demand that appears inconsistent with domestic law or procedures or international human rights laws and standards on freedom of expression;

- Adopt policies and procedures to address how the company will respond in instances when governments fail to provide a written directive/when government demands do not include a written directive, or fail to adhere to domestic/established legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.

The GNI provides a number of comments on these guidelines (referred to as "Application Guidance"). These stress that when possible, companies should seek written demands rather than accept verbal orders; and stipulate that "*Policies and procedures adopted by participating companies will address situations where governments may make demands through proxies and other third parties to evade domestic legal procedures.*"

Further "Application Guidance" adds that "*It is recognized that it is neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on freedom of expression/privacy, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend.*" In our view, when a case is serious ("severe"), and representative of a number of cases, and showing a trend towards undue restrictions or demands, companies should indeed challenge them.

Finally, the Implementation Guidelines recognize in another Application Guidance comment that "*the nature of jurisdiction on the internet is a highly complex question that will be subject to shifting legal definitions and interpretations over time.*" In our recommendations, we try to deal with some aspects of this problem, in particular in relation to demands from law enforcement agencies to companies, ordering them to provide data from their servers, when the latter are situated in other countries.[65]

The GNI Implementation Guidelines also stress (again in line with Ruggie) the need for transparency on the part of companies, as concerns demands made of them to restrict freedom of expression, or access to information, or to disclose personal information. We build on this in own recommendations in relation to transparency.

In addition, the GNI Principles and Implementation Guidelines stress the need for companies to engage with governments and international organisations in the promotion and enforcement of the principles.

Finally, we should mention that GNI provides for a serious system of cooperation between participating companies and other stakeholders, aimed at giving real effect to, and expanding on, the principles and guidelines. These include mechanisms for independent assessment of members' efforts to implement and uphold the GNI Principles.

The GNI instruments provide very helpful assistance, and we build on them in our own recommendations. Before coming to those, however, it is necessary to note the problems in this regard.

Country-level content blocking

Companies providing search engines, blogging platforms, and other ways for users to share information have been under increasing pressure from states to block illegal content. Some of this material already conflicts with companies' Terms of Service. The Content Policy for Google's blogging platform, Blogger, for example, bans "hate speech", "crude content", material that "exploits children", threats of violence, copyright infringement, personal and confidential information, and illegal activities. But many countries have criminalised other types of expression that would be protected under US law (such as genocide denial in European nations, and criticism of the monarchy in Thailand). Google, Microsoft, Twitter and Facebook have all therefore developed systems to block access to specific search results, blogs, tweets, videos, and other media on a country-by-country basis.

While this country-specific blocking is less than ideal from a freedom of expression perspective, it is preferable to having material that is criminal in any one country completely removed from the Internet. Without these mechanisms, companies face being blocked in specific jurisdictions, as well as criminal proceedings against local staff.

Transparency is the main mechanism companies have used to protect against over-blocking. Google, Microsoft and Twitter have developed measures to inform users when material has been blocked, such as notifications on search result pages and greyed-out warnings that "This tweet from @username has been withheld in: Country". User location is determined based on their IP address, although Twitter allows users to select a different location, or to choose "worldwide", thereby avoiding blocks. Google and Twitter also send removal requests for publication and analysis at the Chilling Effects website run by the Electronic Frontier Foundation and several US universities.

After complying for four years with Chinese government demands to filter a wide range of political content from search results, Google decided instead in 2010 to redirect customers from mainland China to their unfiltered site in Hong Kong. Searches for politically sensitive keywords are now blocked by China's national firewall. Google has just started notifying users in mainland China when they search for terms that are known to cause blocking.[66]

It remains to be seen whether governments and courts will be satisfied with country-specific, reactive blocking. If users are made aware that content has been blocked, there are a number of ways they can get around those restrictions.

Twitter says it will refuse to proactively block tweets (based for example on keyword filtering), but Brazilian prosecutors have already applied for an injunction to block tweets reporting on the location of traffic speed traps and checkpoints. British courts frequently issue broad privacy injunctions forbidding the publication of certain private facts, and a UK parliamentary committee recently called for Internet intermediaries to play a bigger role in enforcement. In both cases, a purely reactive approach is unlikely to stop information from spreading quickly. But the effectiveness of more proactive filtering is also unclear, and would be likely to impose very significant constraints on freedom of expression.

2.5 Difficulties in applying the existing and emerging international standards in the digital environment

There are six main points to be made on the question of how new communication technologies can be regulated or managed in order to prevent them being used by states to perpetrate human rights violations (or to stop them from being so used once repression has begun). These six matters have a bearing on a variety of issues discussed later, including our recommendations on practical measures and arrangements that companies and governments can take or make, and on the question of whether, and if so how, the existing arms export control regimes can be used to control those technologies. We have added brief comments to each of these issues, with reference to our discussions elsewhere, and to our recommendations.

The devices we discuss, for interception, blocking, and data mining, by their very nature can be used for a wide variety of purposes. They can support marketing or behavioural advertising; human rights sensitive but not necessarily incompatible purposes (such as police surveillance in the context of a criminal investigation, or more problematic, national security intelligence or anti-terrorist operations); or serious breaches of human rights, such as suspicionless mass surveillance to find, arrest, torture or kill political opponents, or the blocking of political speech, communication and activity.

The distinction between IT products and services is blurring: surveillance and blocking hardware often requires frequent software updates. This may allow the vendor to gain an insight into how the product is used. Sometimes devices can be remotely disabled, especially if explicitly designed with that functionality. It may be possible to build certain functionalities into the products concerned to flag unusual uses, or even to limit uses to what is reasonable in normal, legal, targeted interception. We build some of our recommendations on this.

Interception and blocking technologies are used for repression and to perpetrate serious violations of human rights in situations that have not (yet) deteriorated to the extent of constituting a non-international armed conflict in the sense of Additional Protocol II to the Geneva Conventions, or a clear threat to regional or international peace and security in the sense of the UN Charter. This is relevant to the question of whether arms control/export control arrangements can be used to limit the spread of the technologies this report is concerned with.

The most applicable agreement is the Wassenaar Arrangement, established in 1996 to promote "transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations".[67] As discussed below, these arrangements are generally focused on, or even explicitly limited to, the spread of "arms", "military capabilities", and exports that could threaten regional or international peace and security. Our recommendations therefore also moot the possibility of applying the principles in such arrangements *mutatis mutandis* in cases in which the formal arrangements could not cover the technologies discussed in this report.

These technologies are traded globally and relatively freely. This too is relevant to the application of arms and export controls. The Wassenaar criteria suggest that if a potentially "dual use" item is relatively easily available on the open market, from states that are not part of the Wassenaar Arrangement, or if the export of the item cannot be easily controlled,

or if it cannot be easily specified in sufficiently clear and objective terms, then the item should not be put on the restricted list at all. Again, therefore, our recommendations are that in such cases the relevant principles and processes should be applied *mutatis mutandis* where possible.

Service providers often process and store data outside their customers' jurisdiction (albeit that telecommunications services more often function around domestic servers and infrastructure). In the "offline world", when law enforcement or national security agencies in one country want to obtain access to evidence in another country, they have to go through "Mutual Legal Assistance Treaties" or MLATs. This typically involves a court in the first country requesting a court in the second country to issue an order for the seizure, production and handing over of the materials. It usually involves legal proceedings to ensure that the substantive and procedural rights of all affected persons and entities are protected. MLATs are complex and can be cumbersome in practice.[68] However, by-passing established MLAT processes constitutes an infringement of the sovereignty of the second state, and a negation of the legal rights of interested parties under the laws of that state, especially if those parties are headquartered or established in that state.

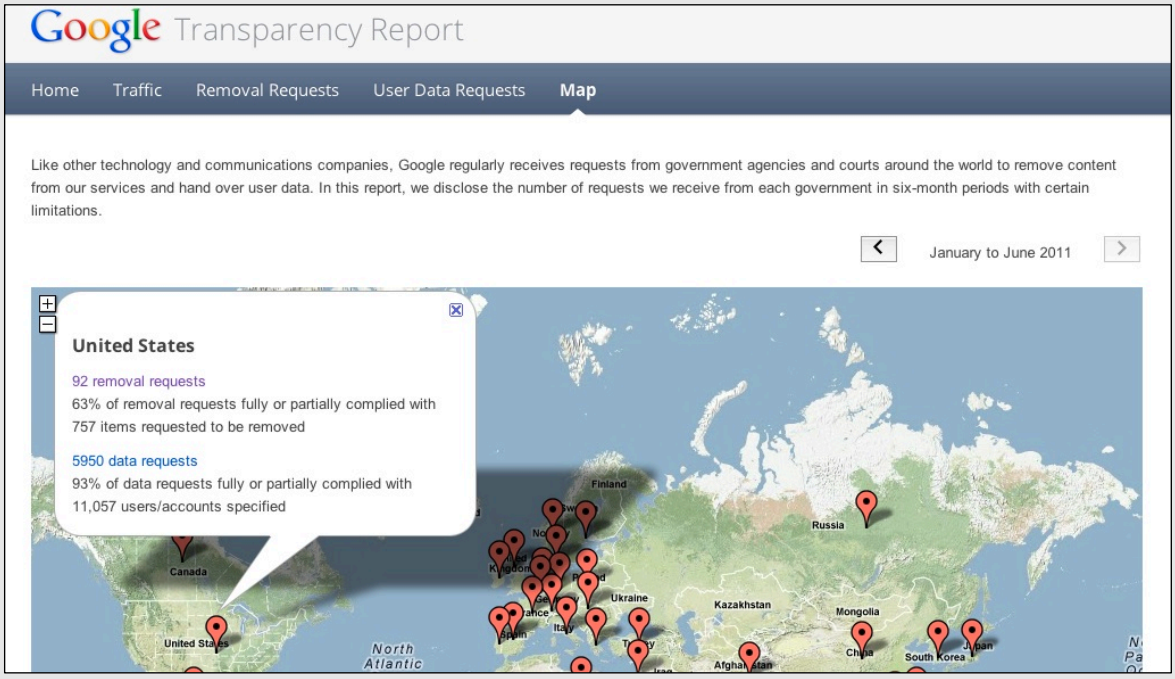
Collecting evidence relating to a suspected offence, or for intelligence purposes, is a form of so-called "enforcement jurisdiction" (as distinct from "prescriptive jurisdiction", which covers the issuing of substantive rules relating to acts). In relevant international law there is a basic principle: "enforcement jurisdiction may not be exercised in the territory of any other state without the consent of that state."[69]

States can of course grant other states the right to exercise enforcement jurisdiction on their territory via treaty. Long-term acquiescence in respect of some specific form of enforcement jurisdiction by many states would come to be recognised as "customary law". However, that cannot yet be said about extracting data from remote servers. We therefore later make proposals that reaffirm the need to abide by established MLAT procedures, yet also recognise that those procedures need to be streamlined and dramatically speeded up, especially in cases such as an immediate risk to life.

Google's transparency report

Like other Internet companies, Google receives requests from governments and courts around the world for user data and to block content. It has played a leading role in improving the transparency of these requests through its Transparency Report service, which shows the number of requests by country in six-month intervals, with details of each request unless the government concerned prohibited full disclosure, and the percentage of requests complied with fully or in part. Google also publishes details of traffic patterns to specific services by region, which allows users to see where access may be blocked, and has recently added information on requests made by copyright owners.

There are some limitations to the statistics. Google excludes requests to takedown child abuse images, which are against the company's own Terms of Service. Individual figures are not made available for countries that have made fewer than 10 content removal requests, since they provide limited information. Similarly, countries that have made fewer than 30 user data requests are excluded, as they might place investigations at risk. Government requests made via the company's public reporting web forms may not identify a government source. Other requests arrive in a range of formats, making it difficult to categorise automatically for statistical purposes.



The data, going back to July 2009, is already revealing interesting patterns in the level and trends of requests, as well as how frequently Google complies with them. US removal requests were relatively stable over this time period, with compliance at around 80%, although with a drop to 63% in the first half of 2011. Pakistan submitted a very small number of requests, none of which were complied with. Brazil was one of the largest submitter of requests, with around 70% complied with. Data for China is largely unavailable, as YouTube was blocked and "Chinese officials consider censorship demands to be state secrets, so we cannot disclose any information about [search] content removal requests for the two reporting periods from July 2009 to June 2010." Google has recently begun notifying Chinese users when their search queries may cause connection issues.

3 Export controls and licensing

There has been widespread criticism of companies in democratic states that have exported products and services to repressive regimes for mass Internet surveillance and censorship. Iran, Syria, Azerbaijan, Belarus, Uzbekistan, China, Bahrain, and recently overthrown regimes in Libya, Tunisia and Egypt, have all blocked critical websites and/or spied on protest movements using such systems.[70]

Many of these tools are "dual use", with legitimate network management and security purposes such as filtering "Denial of Service" traffic and malware on ISP networks or speeding up Web browsing and reducing congestion by caching pages closer to users. They include systems for ISP blocking of customer access to illegal content such as child exploitation, copyright infringing sites or gambling sites, which are mandated or imposed through unofficial government pressure on ISPs in countries including the UK and the Scandinavian nations.[71]

Many democratic nations require that ISPs install surveillance equipment to facilitate the "lawful interception" of communications by intelligence and law enforcement agencies, for example through the US Communications Assistance to Law Enforcement Act of 1994. The democracies' security agencies further use investigative tools to monitor the location of mobile devices and personal computers, access webcams and microphones, and scan messages and voice calls for keywords or known speakers.

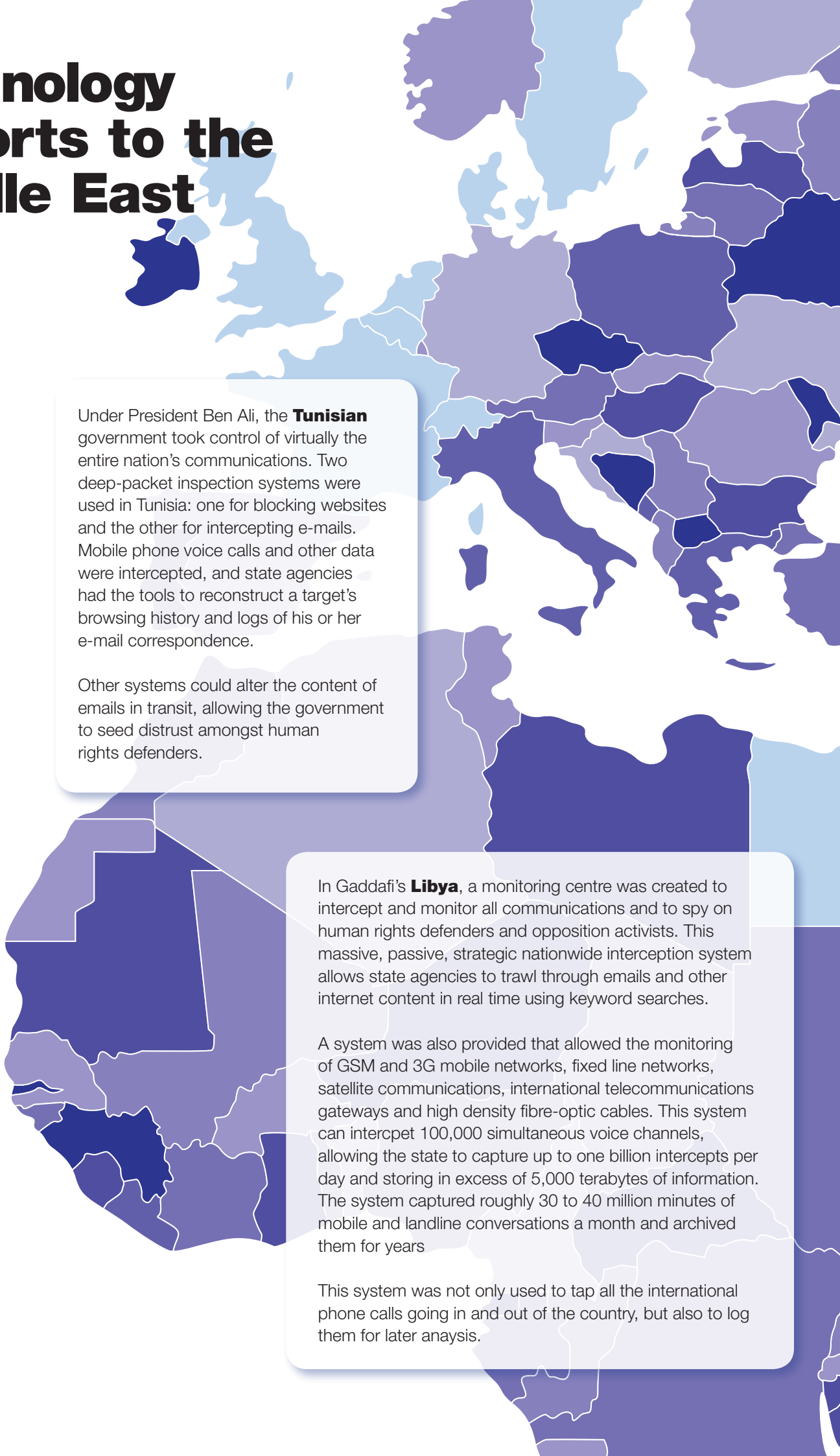
A particular problem from a human rights perspective is that once built, these tools frequently end up in the hands of repressive regimes. A Bloomberg investigation found that by 2007, Nokia Siemens Intelligence Solutions had over 90 monitoring systems installed in 60 countries, while Nokia Siemens Networks spinout Trovicor had surveillance equipment in at least 12 Middle Eastern and North African countries, including Bahrain and Yemen.[72]

Non-democratic countries frequently require ISPs to block customer access to a wide range of websites, especially material critical of the government, or other types of political expression. China's "golden shield" project uses equipment from companies such as Cisco to block material related to the Falun Gong organisation and the 4 June 1989 protests in Tiananmen Square, even though, as Cisco Vice-President Mark Chandler has blogged, "We have never customized our equipment to help the Chinese government – or any government – censor content, track Internet use by individuals or intercept Internet communications".[73] A leaked internal Cisco presentation from 2002 showed that the company had noted the Chinese government's wish to use the "golden shield" to "combat 'Falun Gong' evil religion and other hostiles".[74]

3.1 States' Responsibility to Protect

It is increasingly recognised in international law, especially within the UN system, that states have a "responsibility to protect" their own citizens. Any serious failure by a state to fulfil this duty is a matter of legitimate concern. The international community has the right to take steps against states that seriously fail in this respect, in particular by violently repressing political opposition and indiscriminately attacking civilians and civilian targets, even if there is as such not yet any threat to regional or international security.

Technology Exports to the Middle East



Under President Ben Ali, the **Tunisian** government took control of virtually the entire nation's communications. Two deep-packet inspection systems were used in Tunisia: one for blocking websites and the other for intercepting e-mails. Mobile phone voice calls and other data were intercepted, and state agencies had the tools to reconstruct a target's browsing history and logs of his or her e-mail correspondence.

Other systems could alter the content of emails in transit, allowing the government to seed distrust amongst human rights defenders.

In Gaddafi's **Libya**, a monitoring centre was created to intercept and monitor all communications and to spy on human rights defenders and opposition activists. This massive, passive, strategic nationwide interception system allows state agencies to trawl through emails and other internet content in real time using keyword searches.

A system was also provided that allowed the monitoring of GSM and 3G mobile networks, fixed line networks, satellite communications, international telecommunications gateways and high density fibre-optic cables. This system can intercpet 100,000 simultaneous voice channels, allowing the state to capture up to one billion intercepts per day and storing in excess of 5,000 terabytes of information. The system captured roughly 30 to 40 million minutes of mobile and landline conversations a month and archived them for years

This system was not only used to tap all the international phone calls going in and out of the country, but also to log them for later anaysis.



In **Syria**, a planned system that would have intercepted and stored every email flowing through the country - capturing both domestic and international traffic - was aborted in 2011 after the company involved pulled out, leaving an old system that can only intercept a portion of the country's traffic. The system, which was to use deep-packet inspection probes to monitor email, was to be integrated with the state-owned Syrian Telecommunication Establishment, the nation's main fixed-line operator.

Although this system was abandoned, there are still systems in place to filter and censor the Internet and to record browsing histories.

In **Iran**, state agencies are able to monitor the locations of mobile phones, tracking a target's movements every fifteen seconds and mapping their movements, on at least one major commercial network. Another system can analyze all messages in English, Persian or Arabic for keywords or phrases, store them and flag those caught by filters for review.

Communications monitoring centres have also been used to track and arrest activists.

Yemen monitors the locations of mobile phones, allowing state agencies to track a target's movements and plot the locations on a map.

There is a monitoring centre in **Bahrain** used to monitor phone calls, e-mails, text messages and Voice Over Internet Protocol calls. Some products used by the local security services can also secretly activate laptop webcams or microphones on mobile devices using trojans.

The monitoring centre has the capabilities to change the contents of emails as they pass through the network, use speaker recognition technology to scan phone networks (detecting people who are attempting to stay under the radar by using "burner" phones) and pinpoint people's locations through their mobile phones. The centre can scan traffic in real time for keywords in written and verbal communications for additional analysis.

Egypt acquired trojans and remote infection proxies to infect laptops and mobile phone devices before the fall of the Mubarak regime. This allowed state agencies remote access to the filesystems and webcams of the devices they infected. The tools even allowed them to remotely turn on microphones to surreptitiously record the conversations of pro-democracy defenders.

Mubarak's government also used Deep Packet Inspection technology to monitor web traffic; it is not known whether this equipment is still in use.

US and EU sanctions against repressive regimes such as Iran and Syria already include specific bans on the export of technologies and services that could aid in human rights violations. In April 2012 the US added additional controls on companies that enable those violations, particularly those that "create or operate systems used to monitor, track, and target citizens for killing, torture, or other grave abuses".[75]

Clearly such sanctions should be imposed against other regimes that engage in torture and mass killings, as the European Parliament noted in a non-binding resolution passed on 18 April 2012. However, these alone will not prevent monitoring and censorship tools being acquired and built into the infrastructure of repressive regimes that have not yet reached this stage. One official told us that sanctions are extremely time-consuming to agree (not least due to political sensitivities over significant national exporters), often easy to circumvent, and difficult to extend beyond a small number of targets.

3.2 Dual use controls and the Wassenaar Arrangement

There are extensive international controls on the export of "dual use" technologies with civil and military applications. The main example is the 41-state Wassenaar Arrangement, whose members agree to monitor and control exports of "major or key elements for the indigenous development, production, use or enhancement of military capabilities," and to share information on exports and refusals of exports to non-participating states.

The Wassenaar control list already includes equipment that can be used to intercept mobile phone calls using the GSM standard, although this does not apply to network providers. Human rights groups such as Reporters San Frontières have called for such controls to be extended to surveillance and censorship products and services destined for authoritarian states:

> *The leaders of international companies operating in the new technology domain, especially telecommunications surveillance... should think about their responsibility. Their tools, their equipment and their know-how are being used for criminal purposes... Like the EU regulations on trade in products that could be used for "capital punishment, torture or other cruel treatment," there is now a need to introduce international regulations on the provision of technology that threaten cyber-citizens, to control the export of certain technologies, to create a monitoring body that is independent of governments and to have dissuasive sanctions ready.*[76]

Other parts of the IT industry have been faced with concerns that their products could be used to impose censorship or surveillance in repressive states. For example, the Chinese government proposed in 2009 that "Green Dam Youth Escort" filtering software should be pre-installed on or supplied with all new personal computers. This requirement was made optional after criticism from the public and from PC suppliers. But other states such as Indonesia and Vietnam have raised the possibility of similar mandates.[77]

The Wassenaar controls are only applied to items where the state parties are able "to control effectively the export of the goods." This could be difficult with highly portable communications tools, especially software. For example, in 2011, activist group Telecomix obtained logs from Blue Coat ProxySG web devices installed on the Syrian Telecommunications Establishment backbone network, which were being used for

monitoring and blocking of connections.[78] Blue Coat stated after reviewing these logs that a distributor in the United Arab Emirates had illegally diverted the devices to Syria. That distributor has now been added to the US Department of Commerce's export control list. Blue Coat added: "We are not providing support, updates or other services to these appliances... If our review of the facts about this diversion presents solutions that enable us to better protect against future illegal and unwanted diversion of our products, we intend to take steps to implement them".[79] A technologist told us that there is a thriving second-hand market in equipment that can be used for mass surveillance and blocking, often sold by ISPs in advanced economies as they upgrade their networks, which is perfectly adequate for the networks in use in less industrialised economies.

The Wassenaar concept of "dual use" does not fit fully with human rights protection. The instruments relating to export controls are aimed primarily at preventing threats to global and regional peace and security, including at most non-international armed conflicts in the sense of Additional Protocol II to the Geneva Conventions. Many recent and ongoing situations of serious repression and human rights violations do not fall within this category.[80] "Dual use items" or "goods" are defined as those that can be used for both civil and military purposes (EC Regulations), or as (civilian) goods and technologies that can "enhanc[e] military capabilities" (Wassenaar). Human rights issues are therefore at most matters to be taken into account in assessing whether export restrictions should be imposed, or even whether certain technologies should be classified as "dual use".

However, until and unless an internal situation deteriorates to the extent that large-scale military force is used (as in Syria at the time of writing), many of the technologies we are discussing can already be used to enable widespread repression, contrary to international human rights law, without that use being "military" in the export-control sense. And even if there is a real "military" use of the technologies, under the current export control systems the question of human rights compliance of an importer is at most only one aspect that may be taken into account.

Technology companies have legitimate concerns that export controls will limit access to potentially significant markets, and impose bureaucratic constraints on legitimate sales that may be ineffective against bad actors. The Wassenaar Arrangement specifies that it "will not impede bona fide civil transactions." One civil society expert told us they "have yet to see a workable definition based solely on the tools' capabilities or other attributes that won't either be too narrow or so broad that they undermine the people we're trying to help."

Any controls should therefore be limited to monitoring technology that has very limited legitimate uses - such as mass surveillance equipment that can be used at a national scale to monitor or block very large numbers of simultaneous communications, and "weaponised exploits" that exploit weaknesses in commonly-used software (such as Microsoft Windows or Apple's iOS) for the purposes of undertaking stealthy monitoring.[81] Campaign group Privacy International, for example, suggests controls on items such as "IMSI, MSISDN, IMEI, TMSI interception and monitoring equipment" and "Tactical SMS, GSM, GPS, GPRS, UMTS, CDMA, PSTN and satellite phone interception and monitoring equipment". The European Parliament called in 2011 for a ban on "the granting of general authorisations from the EU for exports to certain countries … of telecommunications technologies for use in connection with a violation of human rights, democratic principles or freedom of speech as defined by the Charter of Fundamental Rights of the European Union, by using interception technologies and digital data transfer devices for monitoring mobile phones and text

messages and targeted surveillance of internet use (e.g. via Monitoring Centres and Lawful Interception Gateways)".[82]

Some categories of very high performance monitoring equipment suitable for mass surveillance may be able to be specified precisely enough to be included. The US already restricts the export of technologies that are "primarily useful" for the "surreptitious interception of wire, oral or electronic communications".[83] A civil society expert told us that bespoke equipment is being made for repressive regimes, including technology such as location tracking, with teams of European engineers on the ground maintaining the technology.

Some software and telecommunications equipment requires frequent updating by the vendor for ongoing functionality, or can be remotely disabled. Where such restrictions can be shown to be effective, the need for export controls on that equipment as a preventative measure is reduced, since usage controls can be put in place at any time. These restrictions can also reduce the circumvention of export controls by the resale of controlled equipment, especially where the end-user needs to connect the equipment to the vendor from an IP address whose geographic location can be determined with reasonable accuracy – although such controls can in themselves be circumvented.

3.3 Protecting tools for activists

One danger of sanctions and export controls is that they block the provision of useful tools to democracy activists. This can happen explicitly, through broad controls such as those applied by the US against countries such as Iran and Syria. But even when those controls are relaxed, the complexity of the controls and the harsh penalties for making a mistake still discourage many companies from allowing the use of their products by anyone in these countries. This has stopped Zimbabwean activists looking for web hosting, Iranians from downloading web browsers and using blogging and open source software sites, and Syrians from using LinkedIn -- even after the US Treasury granted general licenses for the export of communications tools to the latter two countries.[84]

The Obama administration offered further guidance in March 2012 to US companies wanting to provide services to Iranians, but this does not extend to a number of tools useful for activists, such antivirus software, Virtual Private Networking code, or domain names and SSL certificates. The European Parliament resolved in April 2012 that EU policies in this area "should be precise in order to be effective and not to hurt human rights defenders". Marietje Schaake MEP told us that she is campaigning for the EU to set up industry-specific "checkpoints" for companies to go through before setting up business deals in repressive states, which could provide human rights assessments and confidential advice to businesses that would then have certainty under EU law. She also proposes to explore ways in which the EU can support businesses when they face pressure to violate human rights in third countries. Controls equally should not get in the way of other legitimate purposes, such as security research and development.

The Electronic Frontier Foundation offered to help companies navigate the complexity of export licenses, although this offer has yet to be taken up. EFF has also campaigned for such "piecemeal approaches" to be replaced with the removal of all export controls on communications tools and services.[85]

Many activists remain extremely critical of export controls after the attempts of the US government to use them to stop the spread of privacy-protecting encryption software during the 1990s. The most high-profile target was the Pretty Good Privacy (PGP) open source software initially developed by Phil Zimmerman, who became the subject of a three-year criminal investigation by the US Customs Service. This was dropped without charges, and the software became widely available online. This case is a useful demonstration of the limited impact export controls are likely to have on software-only systems, especially where the underlying mathematical algorithms are widely published (and protected as free speech).[86] The authors of "circumvention tools" such as Tor, who have received funding for this purpose from the US State Department, told us they are still having problems getting licences to export those very tools to activists in repressive regimes. Another significant problem is open source software with developers around the world with no clear "owner" or "exporter".

3.4 Transparency and non-Wassenaar producers

Countries outside the Wassenaar Arrangement play an important role in the availability of controlled items. Software giant India is bidding for membership of Wassenaar, with the support of the US. But Chinese companies are developing increasingly sophisticated computing and telecommunications systems, with a Reuters investigation finding that Shenzhen-based ZTE Corporation has supplied Iran's main telecommunications company with surveillance equipment that can "locate users, intercept their voice, text messaging ... emails, chat conversations or web access." The company also appeared to be supplying export-controlled US technology to Iran. [87]

By contrast, in December 2011 Chinese company Huawei decided to scale back its activities in Iran, "by no longer seeking new customers and limiting its business activities with existing customers".[88] This was an illustration that transparency leading to a negative public reaction can be a powerful motivator of company behaviour. A second example is technology companies' reaction to the government of Pakistan's call for tenders on a national Internet blocking system, which required the capability to block 50m web addresses. After a campaign by groups in Pakistan, with support from GNI, Access and others, companies including Cisco, McAfee, Websense, Verizon and Sandvine all pledged not to bid for the work.[89]

The Electronic Frontier Foundation has suggested mechanisms to increase this transparency, including encouraging government bodies and legislatures to "hold hearings, issue subpoenas for documents or testimony and even conduct full investigations." Human rights reporting requirements could be required in government procurements, and in the annual reports of companies of companies doing business with repressive regimes.[90] Companies can carry out much stronger due diligence on customers in repressive regimes, as recommended by the EFF for government sales[91] and promoted by the proposed US Global Online Freedom Act (HR 3605). Even so, one manufacturer told us that after rejecting five sales in one quarter following an internal human rights review, competitors in Europe and China made those sales.

3.5 Technical standards

An area that has so far been less explored is the inclusion of human rights protections in technology standards related to targeted interception and web blocking (backed up by public procurement rules and legal mandates).

The main "lawful intercept" standards have been developed by the European Telecommunications Standards Institute (ETSI), a non-profit organisation with over 700 members from 62 countries. They cover a range of different communications protocols, from mobile phones, cable TV/telephony, emergency communications systems, to e-mail and Internet access. The use of such standards is mandated in many countries.

The companies designing and operating communications equipment could standardise and implement functionality that could be used to limit the use of their equipment outside this legal, targeted interception framework. Explicit limits could be set on the proportion of communications that could be intercepted within a specific device. The production of unalterable audit logs could help with the oversight of the use of the capability (although not enforce its use). Stricter standards could be set for the verification of interception instructions, avoiding the problems encountered in Greece where investigators are still unsure who used LI facilities to wiretap the prime minister and other top officials.[92] One standards expert told us that intercepts could be targeted on specific senders or recipients of communications, but not on broad keyword searches or speaker recognition. While such requirements would not be typical in an ETSI standard, nor is there such a danger of abuse of other typical communications standards requirements.

Web blocking tools do not have equivalent standards to lawful intercept. However, producers of these tools could similarly explore whether standardisation of protections for freedom of expression would be feasible and useful, alongside concrete principles for sales - such as rejecting government customers that wish to use tools to impose filters going beyond the ICCPR on their citizens, as China's "Green Dam Youth Escort" and Pakistan's proposed national firewall would both have done. GNI member Websense has taken such a position.[93] One technologist suggested to us that high-performance blocking systems could be designed that would only accept blocking configurations digitally signed by their manufacturer.

3.6 Civil liability and private rights of action

A further potential remedy is a private right of action for individuals whose human rights are violated using equipment or systems designed for this purpose. Two ongoing cases in the US are attempting to create such a precedent: *Du v. Cisco* in the US District Court of Maryland, and *Doe v. Cisco* in the US District Court for Northern California. The suits have been brought under the federal Alien Torts Statute Act and Torture Victim Protection Act, as well as state law.[94] Yahoo! Inc. settled a similar case in 2007.[95] Cisco has responded that "The lawsuits are inaccurate and entirely without foundation".[96] French human rights groups FIDH and LDH have similarly filed a criminal complaint and an application to join civil proceedings against Amesys with a Paris court, for "being complicit in grave violations of human rights on the basis of extraterritorial jurisdiction".[97]

4 Recommendations

On the basis of our analyses and building on the Ruggie and GNI Principles and Implementation Guidelines, discussed above, we propose the measures set out below as possible practical steps that can be taken to prevent or mitigate human rights violations perpetrated or facilitated by the use globally networked digital technologies.

We have set out our proposals under five headings, addressing companies, governments, intergovernmental organisations, NGOs, and investors. However, as should be clear from the proposals, the strength of any action taken in this respect will depend on positive cooperation between them. Our proposals are tentative: they are put forward as a basis for further discussion, not as fully-fledged prescriptions. But we hope that they add some further flesh to the structures usefully created by the Ruggie and GNI principles.

4.1 Companies

1. Companies should exchange information on legal systems and experiences in specific jurisdictions with other companies, governments, intergovernmental organisations and NGOs. Where such information is sensitive, it can be shared in trusted forums such as GNI. Companies should aggregate and collectively make available public information on their experiences in a format that will shield them from sanctions from authoritarian governments – if necessary, through an independently operating third party to avoid competition concerns. On the basis of such exchanges, GNI members will be able to review and develop the GNI Principles and Implementation Guidelines, and see how they can incorporate the present proposals into them. All of our interviewees were in favour of greater information sharing and transparency, while recognising that this is not on its own a panacea.
2. Before entering a market, companies should assess whether the domestic legal systems and practices conform to international human rights and rule of law requirements. In this, they can draw on information provided by intergovernmental organisations, governments in democratic countries that publish assessments of the human rights situation in various countries, and reputable NGOs. If these indicate that the authorities in the country are involved in human rights abuses, and if the technologies the company is considering selling there could contribute to such repression, it should carefully plan how (and whether) it can make its technology available in a form that minimises the risk of abuse. It should also plan how to respond to legal and extra-legal demands from that government that have human rights implications.
3. Companies should ensure they have a clear understanding with governments about the lawful procedures under which subscriber data can be requested, material blocked, and connections terminated. Where possible they should agree specific points of contact for senior law enforcement, national security and regulatory officials, and mechanisms to check the authorisation of requests from these contacts. One telecommunications company told us that after agreeing such procedures with a government in the Middle East, data requests fell from 16,000 to 4,000 per month.
4. Companies should disclose policies and procedures they have in place to manage human rights risks. They should share and collectively publish aggregate statistics about use of blocking and subscriber data access procedures, unless expressly prohibited from doing

so by statute or the courts. Where such statutes are not clearly in compliance with international law standards, companies should challenge ambiguous demands in the higher courts. They should in all cases keep a detailed record of actions (if only to defend themselves in possible subsequent legal actions). Information about specific cases can be disclosed confidentially when appropriate to “safe harbour" recording schemes.

5. Companies should stipulate in the terms and conditions for the use of their products that they should not be used in violation of international human rights law. This should include speedy mechanisms for dispute resolution in such cases, involving the diplomatic services of the home country of the company. Technical measures for enforcement can include in-built mechanisms to disable, withdraw or stop offering the product or service if and when it is used in clear breach of international human rights law, and when the country that perpetrates these violations has not stopped that illegitimate use after attempts at resolution. Before finalising the supply of a potentially repressive product to a non-democratic country without meaningful human rights protections and the rule of law, companies should seek assurances from, and make arrangements with, the authorities of the state about the protection of human rights, especially during emergencies.
6. If a company notices that a product has been exported to a repressive country without its prior agreement, it should consider disabling the product. This applies *a fortiori* if the unauthorised export is to a country known to perpetrate wide-scale or serious human rights violations.
7. Companies should use “Privacy by Design” principles to reduce the processing and storage of personal data no longer required for a legitimate business purpose, which could later be subject to compelled disclosure. In relation to countries with deficient laws, this may include storing as much data as possible on servers located outside the control of that jurisdiction. Companies’ terms and conditions should specify that user data only be provided to government agencies upon receipt of a legally binding request. Where the company holds data on servers outside the jurisdiction, the company should insist that the host country authorities use the appropriate Mutual Legal Assistance arrangements (bilateral or multilateral MLA treaties) as the only appropriate means of access.
8. If the law enforcement or national security authorities of the host country demand *ad hoc* access to data held by the company in contravention of the host country’s own (normal or emergency) laws, or on the basis of emergency that is invoked in contravention of international human rights law, or in circumstances that suggest that the likely uses of the data will violate international human rights law, the company should challenge the demand before the courts of the host country whenever this is practicable, and resist attempts at access pending full judicial review of the demand.
9. If the host country demands direct access to company data, through the insertion of opaque “black box” interception or access devices, the company should fundamentally consider its provision of the product to the country: such effectively unlimited and uncontrollable access is fundamentally contrary to the basic principles of the rule of law, unless accompanied by a very strong control and oversight regime.[98] If such demands are made in circumstances in which the state in question is perpetrating large-scale or serious human rights violations, it must be assumed that those demands support such

violations. In order to avoid implicating themselves in such violations (and legal liability for complicity in such violations), companies should urgently review their provision of products and services within the country.

4.2 Governments

10. Governments of democratic countries, and their diplomatic missions, should support companies in the implementation of the above proposals. They should assess the human rights situation in the countries with such missions, and share this information with companies thinking about offering products and services in those countries, in particular when there is evidence that widespread or serious human rights violations are or are likely to take place in the country. This assessment should include any emergency laws. Those governments and missions should be able to draw on expert knowledge within their own ministry to this end. One government told us they already included this type of information in a risk register maintained by each embassy. Democratic countries and their diplomatic missions should moreover engage with companies and NGOs in the exchanges of information referred to above.
11. Governments and diplomatic missions should make clear that any serious breach of human rights assurances given to companies will be taken up at a high diplomatic level, and will have serious diplomatic repercussions.
12. Governments should be willing to engage in dispute resolution measures to try and resolve any conflicts over human rights compliance in the use of products sold and supported by companies from their country. They should support companies that feel forced to disable products in the circumstances described above, or to challenge demands from the host country, or to withdraw their product.
13. States should insist that demands for access to data held on their territory should be made only through the applicable Mutual Legal Assistance arrangements (bilateral or multilateral MLA treaties), and that extraterritorial demands for access to data on a server in their jurisdiction would otherwise constitute a violation of sovereignty.[99] Consideration should be given to explicitly backing up such action by the domestic law of the countries concerned, and in the inter-governmental arrangements and treaties referred to below. They should also consider applying civil legal liability to companies that fail to perform due diligence checks, and fail to take measures to prevent, mitigate or end abuse of products for the perpetration of large-scale or serious human rights violations.
14. States should consider including tools that have primary or significant potential uses for human rights violations (such as high-end mass surveillance equipment and weaponised exploits) in “dual use” export control regimes, requiring suppliers to undertake extensive due diligence on end-users before export to or support, maintenance or training for specific repressive regimes.
15. States should formally and explicitly extend the purposes of international arms control agreements from essentially international military security to cover also the protection of human rights - or at least, in the terms of the UN system, to include the aim of preventing or stopping states from failing to fulfil their “responsibility to protect” their own citizens. The Wassenaar Arrangement is the broadest international agreement that

could be used for this purpose - a critical requirement to prevent a “race to the bottom” where suppliers simply move their operations to countries that have not imposed such controls. Until this is achieved, we suggest that many of the Wassenaar rules should be applied *mutatis mutandis* to situations in which states fail to fulfil their “duty to protect” the human rights of their own citizens, or in which this looks likely to happen imminently. The Wassenaar Arrangement requires “The ability to make a clear and objective specification of the item.” The maintenance of a list of controlled items and targeted states would require frequent multi-stakeholder discussion between the Wassenaar states, technology companies, and human rights groups and academics with expertise in the use of these tools for human rights violations.

16. Tools useful for political activism should be more clearly excluded from export controls and sanctions. At a minimum, broad general licences, allowing the export of software and support as well as information, are easier to understand and comply with than a requirement for individual licensing procedures. The Information Security section of the Wassenaar dual-use list could be immediately scrapped as it is now largely obsolete, but still obstructing the distribution of activism tools such as Tor.
17. Transparency is crucial to ensuring that intrusive technologies are used correctly, in line with the standards we have adduced. States should establish oversight and reporting procedures in relation to the use of those technologies, and encourage wide debate on them, including in their legislatures. Meaningful statistics and information should be published to allow the general public to see how, how often, and in what kind of circumstances or cases such technologies are used. Failure by a state to seriously supervise and report on the use of such technologies is a clear indicator of likely abuse, and is thus a factor that companies should take into account in their "due diligence" risk assessments.

4.3 Inter-Governmental Organisations

18. Global and regional IGOs should review the international system relating to Mutual Legal Assistance arrangements (bilateral or multilateral MLA treaties), to address the currently unresolved complex legal issues that arise under them,[100] with a view to support the recommendation we made for governments to confirm that law enforcement and national security agencies in one country should not demand access from a company in that country to the company’s servers and data in another country, but rather, that such demands for access to such data held in the latter country should always be made through the relevant MLA treaty. At the same time, such a review should also address the need to introduce speedy (and in some case, emergency) access to such data under such MLAs, subject to appropriate safeguards. Further research is needed into measures that can increase the responsiveness of MLA requests while protecting human rights and public policy objectives, as well as understanding how to resolve conflict of laws issues that are currently arising – a key issue according to one official we interviewed.
19. Intergovernmental organisations should make clear that countries and regional organisations like the EU may provide incentives to companies that act in accordance with the recommendations made above, and conversely may impose disincentives on companies that act blatantly contrary to those recommendations, e.g., in terms of preferential treatment in trade and contracts, without that being regarded as an

interference in free trade, or contrary to World Trade Organisation principles. US and European calls for restrictions on Internet freedom of expression to be classified as barriers to trade101 should be given speedy consideration by the WTO.

4.4 Non-Governmental Organisations

20. Non-Governmental Organisations are frequently in possession of reliable information on the human rights situation, and on relevant laws and practices, in countries in which companies would like to sell human rights sensitive products. NGOs should engage with such companies if the latter are keen to avoid becoming complicit in human rights violations in those countries, in a way that would not compromise the independence and impartiality of the work of such NGOs. GNI can provide a forum for such engagement.
21. NGOs can play an important role in educating companies about relevant international standards (which as we have shown are complex), and in training company staff in how to deal with human rights concerns in countries in which they operate, and in the carrying out of human rights impact assessments. NGOs can also help to educate activists about using online communications tools safely.
22. NGOs should support, and engage themselves in, efforts to create stronger international law frameworks for the protection of human rights in relation to the sale and support of human rights sensitive products by companies. They should develop and campaign for stronger human rights law standards on how governments demand content removal /blocking and sharing of user data, given that specific governmental actions often have global implications.
23. NGOs should do more to raise public awareness about the roles and responsibilities of ICT companies in protecting people against human rights abuses, and on how to make informed decisions as consumers and users when choosing between ICT products and services. They can also do more to educate people about how to protect themselves against human rights abuses when using ICTs in their daily lives as well as during political crises.

4.5 Investors

24. Socially responsible investors should expect companies to commit to appropriate human rights standards that meet three essential tests. Standards should have operational utility, addressing issues in a concrete, practical way. They should be developed and implemented in a multi-stakeholder process with NGOs, academic experts and other stakeholders. And they should require accountability through public reporting, even if certain details are held back in some extremely sensitive situations.

5 Endnotes

[1] Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council seventeenth session, document A/HRC/17/27, 16 May 2011.

[2] Dunstan Allison Hope, Protecting Human Rights in the Digital Age: Understanding Evolving Freedom of Expression and Privacy Risks in the Information and Communications Technology Industry, BSR, February 2011.

[3] Cf., e.g., Fredrik Laurin, Telco caught colluding with dictators, Index on Censorship, 1 May 2012: "*Nordic Telecom giant TeliaSonera forced to act after evidence that its data has been abused to target, harass and jail activists in Uzbekistan, Azerbaijan and Belarus*."

[4] Evgeny Morozov, The Net Delusion: How Not to Liberate the World, Allen Lane, 2011, pp.9-14.

[5] Freedom House, Freedom on the Net - A Global Assessment of Internet and Digital Media, 2011, at http://www.unhcr.org/refworld/docid/4dad59042.html.

[6] See in particular the information provided by the OpenNet Initiative at http://opennet.net/: "*ONI's mission is to identify and document Internet filtering and surveillance, and to promote and inform wider public dialogues about such practices*." See publications *Access Denied*, *Access Controlled*, and *Access Contested* and country profiles.

[7] Peter Sommer, Can we separate "comms data" and "content" – and what will it cost? Scrambling for Safety, London School of Economics, April 2012, at http://scramblingforsafety.org/2012/sf2012_sommer_commsdata_content.pdf.

[8] See Ian Brown & Douwe Korff, *Social Media and Human Rights*, in Human Rights and a Changing Media Landscape, Council of Europe Publishing, December 2011, pp. 175 – 206. Note that although the systems may be relatively easy to by-pass, this will often flag up the individuals doing this, and expose them to repressive actions on the part of the authorities.

[9] Most recently see Freedom on the Net, note 5; The Net Delusion, note 4; Richard Fontaine and Will Rogers, Internet Freedom: A Foreign Policy Imperative in the Digital Age, Centre for a New American Security, 2011; Reporters Without Borders, Enemies of the Internet, 2010, at http://en.rsf.org/IMG/pdf/Internet_enemies.pdf; C. Callanan, M. Gercke, E. De Marco and H. Dries-Ziekenheiner, Internet blocking: balancing cybercrime responses in democratic societies, Aconite Internet Solutions, 2009; and Rebecca MacKinnon, Consent of the Networked, Basic Books, 2012.

[10] See Douwe Korff, The Right to Life: A guide to the implementation of Article 2 of the European Convention on Human Rights, Council of Europe Human Rights Handbook No. 8, 2006, in particular pp. 59 – 85. See also the quote from a UN Fact Sheet at the beginning of section 2.3.

[11] Cf. the UN Convention on the Rights of the Child, 1989 (in force since 1990).

[12] Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 28 January 2003, CETS No. 189.

[13] London Assembly, Report of the 7 July Review Committee, Greater London Authority, June 2006, s.3.12.

[14] Home Office, Protecting the Public in a Changing Communications Environment, Cm 7586, The Stationary Office, April 2009, p.8.

[15] Nokia Siemens Networks, Statement to the Public Hearing on New Information Technologies and Human Rights, 2 June 2010, at http://www.nokiasiemensnetworks.com/news-events/press-room/statement-to-the-public-hearing-on-new-information-technologies-and-human-rights.

[16] James Bamford, The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America, 2008, Doubleday and The NSA Is Building the Country's Biggest Spy Center (Watch What You Say), Wired, 15 March 2012; Emma Draper, Round-up: Scrambling for Safety 2012, Privacy International, at https://www.privacyinternational.org/blog/round-up-scrambling-for-safety-2012. When we discussed this with officials from a major Western country, it was not denied that the security agencies of that country might have an interest in certain states using exported "black boxes". The agencies could conduct surveillance through the company and/or vulnerabilities in the systems concerned.

[17] The tests set out here are common to all the main international human rights treaties, but most developed under the European Convention on Human Rights. For a somewhat longer overview of the details of these tests, see: Douwe Korff, The Standard Approach Under Articles 8 – 11 ECHR and Article 2 ECHR, at http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf. Cf. also the Office of the UN High Commissioner for Human Rights, Human Rights, Terrorism and Counter-Terrorism, HCHR Fact Sheet No. 32, 2008, pp. 23 – 26. These basic standards are also reflected in Part I of the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, and in the Johannesburg Principles on National Security, Freedom of Expression and Access to Information.

[18] Cf. the Johannesburg Principles, Principle 1.1(b): "*The law should provide for adequate safeguards against abuse, including* ***prompt, full and effective judicial scrutiny*** *of the validity of [any] restriction by an* ***independent court or tribunal***." (emphasis added)

[19] Human Rights Committee, General Comment No. 31 on the Nature of the General Legal Obligation Imposed on States Parties to the [International Covenant on Civil and Political Rights], 29 March 2004 (2187th meeting), UN Doc CCPR/C/21/Rev.1/Add. 13 of 26 May 2004, para. 8.

[20] *Ibid.*, para. 10. On the duties of companies themselves to respect and protect the rights of their customers, see section 2.4.

[21] The most important "non-derogable" rights are freedom from torture and the right to life (except that acts that result in deaths but that are in accordance with the Geneva Conventions and its Additional Protocols ["lawful acts of war"] are *ipso facto* regarded as

not constituting violations of the right to life: see Article 15(2) ECHR; the same is implied in the ICCPR). Under the ICCPR, freedom of thought, conscience and religion is also non-derogable (although it may be limited under the normal rules). Finally note that, as discussed in the text, the general prohibition of discrimination in the ICCPR is also made non-derogable, in respect of the most important grounds for discrimination.

[22] Article 15(1) ECHR. The ICCPR only has: "*In time of public emergency which threatens the life of the nation*" (Art. 4(1)), but this is read as clearly also including a time of war.

[23] See the UN Fact Sheet No. 32, note 17, pp. 37 – 38.

[24] Human Rights Committee, General Comment No. 5 on *Derogation of Rights (Article 4)*, 31/07/1981; Human Rights Committee, General Comment No. 29 on *States of Emergency (Article 4)*, 31/08/2001.

[25] Note 17. The summary of the standards applicable in times of emergency can be found on pp. 26 – 29 of the Fact Sheet.

[26] The Siracusa Principles were contained in an Annex to a *Note verbale* from the Dutch government to the UN Commission on Human Rights, dated 24 August 1984, and subsequently in UN Document E/CN.4/1985/4 of 28 September 1984. The Paris Minimum Standards were adopted at the 61st Conference of the International Law Association, held in Paris from August 26 to September 1, 1984. They were published in AJIL, October 1985. The Johannesburg Principles were adopted on 1 October 1995 by a group of experts in international law, national security, and human rights convened by ARTICLE 19, the International Centre Against Censorship, in collaboration with the Centre for Applied Legal Studies of the University of the Witwatersrand, in Johannesburg. Although none of these three documents are binding or constitute formal legal interpretations of the law, they chime with the approach taken by the Human Rights Committee and other international judicial and quasi-judicial human rights bodies. Moreover, the first two are explicitly referred to in General Comment No. 29 (See the last sentence of para. 10, and footnote 6 to which it refers.) while the third (the Johannesburg Principles) have been endorsed by Mr. Abid Hussain, the UN Special Rapporteur on Freedom of Opinion and Expression, in his reports to the 1996, 1998, 1999 and 2001 sessions of the United Nations Commission on Human Rights, and referred to by the Commission in their annual resolutions on freedom of expression every year since 1996. All three may therefore be taken as authoritative by companies trying to comply with the GNI Principles.

[27] The main UN documents can be found at: http://ap.ohchr.org/documents/dpage_e.aspx?m=134. Information on the main activities of the Council of Europe in this respect can be found at http://www.coe.int/what-we-do/rule-of-law/terrorism. See also the following pages with links to relevant conventions and other texts: http://www.coe.int/t/dlapil/codexter/conventions_en.asp, http://www.coe.int/t/dlapil/codexter/otherTexts_en.asp. For the activities of the European Union, see the EU Council website: http://www.consilium.europa.eu/policies/fight-against-terrorism?lang=en. The main EU documents in this area are available at: http://www.consilium.europa.eu/policies/fight-against-terrorism/documents?lang=en. See also the website of the EU Counter-Terrorism Co-ordinator, at: http://www.consilium.europa.eu/policies/fight-against-terrorism/eu-counter-terrorism-co-ordinator?lang=en. Cf. also section 4.5 of the EU's "*Stockholm Programme*", at:

http://register.consilium.europa.eu/pdf/en/10/st05/st05731.en10.pdf. One aspect of this programme is the pursuit by the EU, through the UN, of the drafting and adoption of a Comprehensive Convention on International Terrorism (Stockholm Programme, p. 87).

[28] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin - Ten areas of best practices in countering terrorism, Human Rights Council, Sixteenth Session, UN Document A/HRC/16/51, 22 December 2010. The first report by Martin Scheinin's successor as Special Rapporteur, Ben Emmerson, will be submitted to the HR Council's twentieth session, later in 2012.

[29] Fact Sheet No. 32, note 17.

[30] Council of Europe, Human rights and the fight against terrorism: The Council of Europe Guidelines, 2005.

[31] Note 26.

[32] As the UN Special Rapporteur on human rights and terrorism put it: *"The adoption of overly broad definitions of terrorism ... carries the potential for deliberate misuse of the term – including as a response to claims and social movements of indigenous peoples – as well as unintended human rights abuses. Failure to restrict counter-terrorism laws and implementing measures to the countering of conduct which is truly terrorist in nature also pose the risk that, where such laws and measures restrict the enjoyment of rights and freedoms, they will offend the principles of necessity and proportionality that govern the permissibility of any restriction on human rights."* (Ten areas of best practices in countering terrorism, note 28, para. 26). Indeed, we would go somewhat further than the Special Rapporteur, and feel that applying anti-terrorist measures to such acts - i.e., to acts that are not "truly terrorist in nature" - is *prima facie* disproportionate and unnecessary - and thus in violation of international human rights law.

[33] Ten areas of best practices in countering terrorism, note 28, para. 21.

[34] *Idem*, para. 28.

[35] The definition in the Draft UN Comprehensive Convention on International Terrorism reads as follows (emphasis added): "Any person commits an offence within the meaning of this Convention if that person, by any means, unlawfully and intentionally, causes: Death or serious bodily injury to any person; or Serious damage to public or private property, including a place of public use, a state or government facility, a public transportation system, an infrastructure facility or the environment; or **Damage to property**, places, facilities, or systems referred to in paragraph1 (b) of this article, resulting or likely to result in **major economic loss**, when the purpose of the conduct, by its nature or context, is to intimidate a population, or to **compel a government** or an international organization **to do or abstain from doing any act**." Note that it is precisely because no agreement on this definition could be reached that the drafting is deadlocked. On some of the difficulties relating to the definition see, e.g., Innocent Maja, Defining International Terrorism in Light of Liberation Movements, July 2008, at http://www.nyulawglobal.org/Globalex/International_terrorism&liberation_movements.htm).

[36] See the comments in the UN Fact Sheet No. 32, note 17, that "Overly vague or broad definitions of terrorism may be used by states as a means to cover peaceful acts to protect inter alia labour rights, minority rights or human rights or, more generally, to limit any sort of political opposition." (p. 40); and that "Too wide or vague a definition [of terrorism, terrorist acts and terrorist groups] may lead to the criminalization of groups whose aim is to peacefully protect, inter alia, labour, minority or human rights." (p. 44). Cf. also p. 24 of the Fact Sheet, under the heading "(b) In the pursuance of a legitimate purpose".

[37] *Idem*., p. 43. See also the reference to the points made by the UN Special Representative of the Secretary-General in Human Rights Defenders in that respect, on p. 44. Cf. also Principle 2(b) of the Johannesburg Principles.

[38] *Idem*, para. 32. The Council of Europe Convention on the Prevention of Terrorism 2005, CETS No. 196. See also the UN Fact Sheet No. 32, note 17, which stresses that "*Prohibiting incitement to terrorism must therefore be limited to what is actually required to protect national security or public order*", and must always remain proportionate to those aims (p. 26).

[39] Practice 9. *Core elements of best practice in the listing of terrorist entities*, point 1, in para. 35.

[40] Cf., from our own experience: Aspects of the law regarding freedom of expression in the Federal Republic of Germany (1983), later used (with Korff's trial observation report on the case against *Haag et al.*) in the Amnesty International publication Prosecution for the exercise of the right to freedom of expression in the Federal Republic of Germany, AI Document EUR 23/02/85, London, 1985; Criminal-legal restrictions on freedom of expression in Israel and the Occupied Territories (1986), used in an AI Submission to the Israeli government that year. On the German situation in the 1970s and early 80s, see in particular also chapter 4, *Criminal Law as a Weapon/Das Strafrecht als Kampfmittel*, in Sebastian Cobler, Law, Order and Politics in West Germany, Penguin, 1978 (translation of Die Gefahr geht von den Menschen aus: der vorverlegte Staatsschutz, Rothbuch, 1976). These are just examples of the general tendency of anti-terrorist or emergency laws over time spreading out (or being brought forward) to cover all kinds of actions that are manifestly not "of a truly terrorist nature".

[41] UN Fact Sheet No. 32, note 17, section E, pp. 37 – 38, with references to statements by the UN Committee on the Elimination of Racial Discrimination, the Inter-American Commission on Human Rights, the European Commission against Racism and Intolerance, and the European Union Network of Independent Experts on Fundamental Rights.

[42] Report of the independent expert on the protection of human rights and fundamental freedoms while countering terrorism, Robert K. Goldman, submitted to the Commission on Human Rights by the High Commissioner for Human Rights, UN Document E/CN.4/2005/103 of 7 February 2005.

[43] UN Fact Sheet No. 32, note 17, section I, p. 44.

[44] COE Guidelines, note 30, section VI, *Measures which interfere with privacy*, point 1, on p. 11, emphasis added. See also the summary of the case-law of the European Court of Human Rights in this area, on pp. 21 – 22. The UN Fact Sheet No. 32, note 17, deals with the same issues of "*Surveillance, data protection and the right to privacy*" in section J, pp. 45 – 46, but

without adding much to the general rules regarding lawfulness, legitimate aim, necessity and proportionality.

[45] Protection of human rights and fundamental freedoms while countering terrorism, UN Document A/61/267 of 16 August 2006.

[46] See Harris, O'Boyle & Warbrick, Law of the European Convention on Human Rights, 2nd. ed. (2009), Chapter 1, section 5, *Negative and Positive Obligations and* Drittwirkung, in particular pp. 19 – 21.

[47] 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*, UN Human Rights Council Document A/HRC/17/31, 21 March 2011.

[48] Corporate Responsibility to Respect Human Rights Sector Guidance Project, ICT Sector Discussion Paper for Public Comment, Institute for Human Rights and Business and Shift, 24 May 2012, at http://www.ihrb.org/pdf/roundtable-discussion-papers/ICT-Sector-Roundtable-Discussion-Paper-For-Public-Comment.pdf.

[49] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie: *Protect, Respect and Remedy: a Framework for Business and Human Rights*, UN Human Rights Council Document A/HRC/8/5, 7 April 2008. In this report, the Special Representative rightly stresses that: "*The duty to protect is well established in international law and must not be confused with the concept of the "responsibility to protect" in the humanitarian intervention debate.*" (par. 9, note 5, p. 4)

[50] See the Ruggie Principles, Part I, *The state duty to protect human rights* (paras. 1 – 10 of the Principles).

[51] *Idem*., Part II, *The corporate responsibility to respect human rights*, para. 11 (commentary on the first "foundational principle"), emphasis added.

[52] *Idem*.

[53] *Idem*., para. 23 (commentary on "Issues of context"), emphasis added.

[54] *Idem*., Part II, section B, paras. 16 – 24.

[55] *Idem*., para. 17, emphasis added.

[56] *Idem*.

[57] *Idem*., Part II, section B, para. 17 (commentary on the "human rights due diligence" principle), emphasis added.

[58] *Idem*., Part II, section B, paras. 18 and 19, emphasis added.

[59] *Idem*., Part II, section B, para. 21, emphasis added.

[60] *Idem*.

[61] See the principles quoted in the text, and also the more general stipulation in the Preamble to the GNI Principles that: "*Information and Communications Technology (ICT)*

*companies have the **responsibility to respect and protect** the freedom of expression and privacy rights of their users*" (emphasis added).

[62] GNI Principles, Principles 2 and 3.

[63] See Principle 4: Responsible Company Decision Making, Principle 5: Multi-stakeholder Collaboration.

[64] For some reason, these matters are spelled out somewhat differently, and in more or less detail, in the different sections dealing with freedom of expression and privacy. In our shortened summaries or paraphrases, we have brought them together (with emphasis added), and have omitted comments in the Implementation Guidelines referred to as "*Application Guidance*". Rather, we deal with those comments separately later in the text.

[65] In another context, we have addressed the question of the application of domestic law restrictions on freedom of expression to expressions made on websites registered in other countries: see Human Rights and a Changing Media Landscape, note 8. However, that is a separate question from the ones relating to companies' duties and responsibilities.

[66] Google, *Better search in mainland China*, Inside Search, 31 May 2012, at http://insidesearch.blogspot.co.uk/2012/05/better-search-in-mainland-china.html.

[67] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies Guidelines & Procedures, including the Initial Elements (as amended and updated in December 2003 and July 2004), WA Secretariat, Vienna, at http://www.wassenaar.org/2003Plenary/initial_elements2003.htm.

[68] See footnote 92, below.

[69] Vaughan Lowe, Chapter 10 - Jurisdiction, Section III – The Fundamental Principles Governing Enforcement Jurisdiction, in: Malcolm Evans (Ed.), International Law, 1st ed., OUP, 2003, p. 351.

[70] Paul Sonne and Margaret Coker, *Firms Aided Libyan Spies*, Wall Street Journal, 30 August 2011; Vernon Silver and Ben Elgin, *Torture in Bahrain Becomes Routine With Help From Nokia Siemens*, Bloomberg, 22 August 2011; Vernon Silver, *H-P Computers Underpin Syria Surveillance*, Bloomberg, 18 November 2011; Leila Nachawati, *Blue Coat: US technology surveilling Syrian citizens online*, Global Voices Advocacy, 10 October 2011; Cindy Cohn, Trevor Timm and Jillian York, Corporations Can Avoid Assisting Repressive Regimes, Electronic Frontier Foundation, 17 April 2012, at https://www.eff.org/sites/default/files/filenode/human-rights-technology-sales.pdf; The Local, *TeliaSonera 'profits by helping dictators spy'*, 18 April 2012.

[71] Internet blocking: balancing cybercrime responses in democratic societies, note 9.

[72] Silver and Elgin, *idem*.

[73] Mark Chandler, Cisco Supports Freedom of Expression, an Open Internet and Human Rights, Cisco Blog, 6 June 2011, at http://blogs.cisco.com/news/cisco-supports-freedom-of-expression-an-open-internet-and-human-rights/.

[74] Cisco Systems, Overview of the Public Security Sector, 2002, slide 57, at http://www.wired.com/images_blogs/threatlevel/files/cisco_presentation.pdf.

[75] The White House, Fact Sheet: A Comprehensive Strategy and New Tools to Prevent and Respond to Atrocities, 23 April 2012, at http://www.whitehouse.gov/the-press-office/2012/04/23/fact-sheet-comprehensive-strategy-and-new-tools-prevent-and-respond-atro.

[76] Reporters without Borders, Companies that cooperate with dictatorships must be sanctioned, 2 September 2011, at http://en.rsf.org/companies-that-cooperate-with-02-09-2011,40914.html.

[77] Hope note 2 p.21.

[78] Nachawati note 70.

[79] Blue Coat, Update on Blue Coat Devices in Syria, 15 December 2011, at http://www.bluecoat.com/company/news/statement-syria.

[80] *Prosecutor v. Ramush Haradinaj et al.*, The International Criminal Tribunal for the Former Yugoslavia and the Threshold of Non-International Armed Conflict in International Humanitarian Law, ASIL Insights, Vol. 12, Issue 7, 23 April 2008, at http://www.asil.org/insights080423.cfm. Note however that the Security Council has over the last decades become more willing to recognise the existence of a threat to international peace and security, and indeed to authorise the use of force in such contexts. As Christine Gray notes: "The Security Council has not [only] authorized force against an aggressor state, but it has also authorized force in internal conflicts, sometimes in response to non-cooperation with UN-brokered cease-fires; to secure the delivery of humanitarian aid in Somalia and in Yugoslavia; to protect safe havens and enforce no-fly zones in Bosnia-Herzegovina; to restore democracy in Haiti; to protect a refugee camp in Rwanda …" (Christine Gray, *The Use of Force in International Law*, in: Malcolm Evans [Ed.], International Law, 1st ed., 2003, p. 609). Still, there are many situations in which the SC did not act, or recognised the existence of a threat to international peace and security. There have, for instance, been no Security Council Resolutions under Chapter VII of the Charter (which deals with international peace and security) in respect of Uzbekistan - one of the most repressive regimes in the world.

[81] Andy Greenberg, *Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits*, Forbes, 9 April 2012.

[82] 2008/0249(COD) - 27/09/2011 Text adopted by European Parliament, 1st reading/single reading.

[83] 18 US Code § 2512, Export Control Classification Number 5D980 and 5E980.

[84] Cindy Cohn and Jillian York, "Know Your Customer" Standards for Sales of Surveillance Equipment, Electronic Frontier Foundation, 24 October 2011, at https://www.eff.org/deeplinks/2011/10/it's-time-know-your-customer-standards-sales-surveillance-equipment.

[85] Idem.

[86] Whitfield Diffie and Susan Landau, Privacy on the Line: The Politics of Wiretapping and Encryption, MIT Press, 1999.

[87] Steve Stecklow, *Chinese firm helps Iran spy on citizens*, Reuters, 22 March 2012.

[88] *Ibid*.

[89] Maija Palmer, *Technology groups shun Pakistan firewall*, Financial Times, 14 March 2012.

[90] Corporations Can Avoid Assisting Repressive Regimes, note 70.

[91] Cohn, Timm and York, note 70.

[92] Vassilis Prevelakis and Diomidis Spinellis, *The Athens Affair*, IEEE Spectrum, July 2007.

[93] Websense, Websense Policy on Government-Imposed Censorship, 2011, at http://www.websense.com/content/censorship-policy.aspx.

[94] John Markoff, *Suit Claims Cisco Helped China Pursue Falun Gong*, New York Times, 22 May 2011, at http://www.nytimes.com/2011/05/23/technology/23cisco.html.

[95] Sui-Lee Wee, *Insight: Cisco suits on China rights abuses to test legal reach*, Reuters, 8 September 2011.

[96] Chandler, note 73.

[97] FIDH and LDH file a complaint concerning the responsibility of the company AMESYS in relation to acts of torture, 19 October 2011, at http://www.fidh.org/FIDH-and-LDH-file-a-complaint.

[98] COE Commissioner for Human Rights, Issue Paper on Protecting the right to privacy in the fight against terrorism, 2008, in particular the bullet-points in section 7, Conclusions, p. 14. Cf. also the discussions of the supervisory systems over surveillance in the UK and Germany, in the ECHR Cases of *Weber and Saravia v. Germany* (Admissibility Decision on Application no. 54934/00, 29 June 2006) and *Liberty and Others v. the United Kingdom* (Judgment of 1 July 2008).

[99] Cf. the recent report on *US subpoenas on private companies holding EU citizens' data*, in the EDRi weekly report of 27 April 2012: "*Commissioner Reding indicated that the [European] Commission considered that when a law enforcement authority in the US realises that necessary information is outside its jurisdiction, the appropriate channel to obtain the data transfer should be the cooperation mechanisms that are in place with EU Member States where that data are located. Such instruments are, among others, the bilateral Mutual Legal Assistance agreements and, more specifically, the EU-US Mutual Legal Assistance agreement. She added that outside the currently established channels, when replying directly to requests originating by US authorities, companies may be in breach of national rules implementing the Directive 95/46/EC.*"

[100] See Kate Westmoreland, Sharing Evidence across Borders: the Human Rights Challenge, 2012 (forthcoming).

[101] Cynthia Liu, *Internet censorship as a trade barrier: a look at the WTO consistency of the great firewall in the wake of the China-Google dispute*, Georgetown Journal of International Law 42(4) pp. 1199-1240, June 2011.