Global Network Initiative

Opening the Lines

A Call for Transparency from Governments and Telecommunications Companies

A report by Chris Tuppen

www.globalnetworkinitiative.org

ABOUT THE REPORT

This report was commissioned and funded by the Global Network Initiative (GNI) and written by Chris Tuppen. The report has been informed by a number of confidential, wide-ranging discussions with people associated with the telecommunications industry. The author would like to thank everyone who contributed their time, expertise and perspectives.

Many aspects of today's telecommunication infrastructure are highly complex, especially with respect to the Internet. Every attempt has been to make this report both factually correct and accessible to a non-technical audience. However, it is recognised that the simplification process may have missed some issues that are critical to a full understanding of the surveillance technology employed.

The review of legislation was undertaken for GNI by Cullen International, for the EU, Sweden and the UK in March 2012 and Russia in May 2013.

The views expressed in this report are those of its author and do not necessarily reflect those of the Global Network Initiative.

About the Author

Chris Tuppen is senior partner of Advancing Sustainability LLP, an Honorary Professor at Keele University and Visiting Professor of Smart Technologies at University Campus Suffolk. He was previously BT's Chief Sustainability Officer.

He has served on the boards of CSR Europe and BSR, and chaired the Global e-Sustainability Initiative. He was co-editor of the report SMART 2020 – Enabling the Low Carbon Economy in the Information Age.

He is currently a member of the Executive Board of the Prince of Wales Accounting for Sustainability project, a member of the NHS and BBC Sustainability Advisory Groups, a Director of the Aldersgate Group, and a member of the Green Economy Pathfinder Board of the New Anglia LEP.

About the Global Network Initiative

The Global Network Initiative (GNI) is a multi-stakeholder group of companies, civil society organisations (including human rights and press freedom groups), investors and academics dedicated to protecting and advancing freedom of expression and privacy in the Information and Communications Technology (ICT) sector. To learn more, visit **www.globalnetworkinitiative.org**.

TABLE OF CONTENTS

INTRODUCTION FROM GNI EXECUTIVE DIRECTOR

In our digitally connected age, when the number and types of communications connections are growing exponentially, managing the tensions between national security and rights to freedom of expression and privacy is a hotly contested issue. This report examines and explains the particular issues and challenges for telecommunications companies dealing with requests from governments.

Of course governments pursuing legitimate responsibilities for national security and law enforcement face real challenges. But as the worldwide reaction to communications surveillance by the U.S. government makes clear, the necessity and proportionality of surveillance measures are far from resolved. Moreover, the lack of transparency around national security communications surveillance poses a particular problem, not just in the United States but around the world. In his most recent report UN special rapporteur Frank La Rue writes, "In order to meet their human rights obligations, States must ensure that the rights to freedom of expression and privacy are at the heart of their communications surveillance frameworks."

This report grew out of research conducted for the Global Network Initiative on the particular freedom of expression and privacy challenges in the telecommunications industry beginning well before this topic hit international headlines.

Written for a non-technical audience, the report illustrates the types of requirements companies face and how they can respond in responsible ways. It doesn't cover how the commercial operations of telecommunications companies can impact human rights or assess the specific cost implications of some of the recommendations made in the report.

To provide practical insight into the legal environment that telecommunications companies face, we commissioned a study focused on the laws and regulations in place in the following settings: the European Union, Russia, Sweden and the United Kingdom. There were many common features in the legal frameworks and the powers available to governments in the countries covered in the study, but differences existed in the approach taken to transparency, accountability and governance. The markets covered in the study were all relatively mature and there could be significantly different issues in less developed markets. We hope this report spurs additional research that examines these issues in other countries.

GNI was formed in response to these issues, providing a framework for responsible company decision-making rooted in universal human rights standards. We aim to create a global standard for freedom of expression and privacy in the ICT sector. Earlier this year we announced a two-year collaboration with eight globally operating telecommunications companies who have formed an industry dialogue to work on these issues. The unresolved issues detailed in this report can only be addressed through greater transparency and accountability from companies and governments alike.

Telecommunications companies play an essential role facilitating the free flow of information around the world. Their distinctive origins and relationship with governments are important to acknowledge when considering how they can address freedom of expression and privacy issues.

Susan Morgan
Executive Director
GNI

EXECUTIVE SUMMARY

The conceptual foundation reference for human rights, and its subsequent basis in international law, is the Universal Declaration of Human Rights first adopted by the UN in 1948. More recently the UN has addressed the application of human rights in an online world. This paper is concerned with the human rights implications arising from government requirements placed on telecommunications companies to intercept and block traffic.

For much of the 20th century phone calls were in analogue form and physically switched across the network. Most of the time this made it very easy to listen in. Today the intercept techniques employed by the police and security services use highly sophisticated technology and the way interception happens is often undisclosed for obvious reasons.

Few would criticise a government's legitimate use of Information and Communications Technology (ICT) in fighting crime and catching genuine criminals. The same technology can also be abused. When that happens, the telecommunications industry carries a significant reputational risk of becoming associated with human rights abuses. In principle companies can challenge governments and in exceptional circumstances could even consider exiting countries in protest but, as the report explains, this carries many considerations.

As the penetration of phones in developed economy markets has reached near saturation levels, many operators have invested in emerging economies. This has often taken them into unfamiliar territories with a very high-risk environment with regard to human rights infringements. When this happens the risk of being associated, if not complicit, with human rights infringements is higher, and higher still if any in-country partners are fully or partly owned by the state.

Matters of regulation, governance and technical protocols and standards are essential for the smooth working of the entire communication system. The related organisations range from global bodies such as the International Telecommunication Union (ITU) and the World Wide Web Consortium (W3C), through regional standards bodies, to national regulatory authorities. In addition a whole range of legislation is applied by nation states.

This report has looked in detail at legislation from the EU, Russia, Sweden and the UK. Although this is a somewhat limited set, it has been interesting to note the similarity of basic legislation that allows the state to intercept and block traffic. However, there are differences in the detail of the legislation and in its implementation that can indicate different levels of risk exposure for a telecommunications company. Important issues to consider are:

1. **Transparency** – is the state clear about what actions it can legitimately undertake?
2. **Rights of Appeal** – do telecommunication companies have a right to appeal against state interventions?
3. **Accountability** – does the state publish statistics regarding its use of intercept and blocking?
4. **Behaviour** – is there evidence, anecdotal or otherwise, that gives cause for concern?

The report explores the following state interventions in some detail: routing and traffic data; targeted intercept; mass intercept; targeted blocking; and mass blocking. For each case the report considers: the technology involved; the legal context for each country of operation; and the extent to which the government has direct access or is dependent on the service provider to allow access.

In the case of state action, international human rights law recognises that there will be limited occasions when the usual protection to freedom of expression and freedom of information and privacy can be suspended.[1] When this happens a telecommunications company can find itself in a position of having to take decisions with implications for individual rights with conflicting stakeholder views, or conflicting interpretations of the law, or even, of being required by state officials to circumvent local law.

1 See Ian Brown and Douwe Korff, *Digital Freedoms in International Law: Practical Steps to Protect Human Rights Online*, available at https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf.

It may be possible to challenge a government's demands in such as situation. However, many companies have been reluctant to do this, often justifiably in order to ensure the safety of their own employees. Alternatively a company could make a voluntary withdrawal from the country, but this comes with many disadvantages. To minimise their risk in such situations companies are recommended to follow relevant guidelines such as the GNI Principles on Freedom of Expression and Privacy and embrace increased levels of transparency. In particular companies are recommended to establish a set of written processes covering: bidding for a new, or renewal of an existing, operating licence; handling requests for traffic or routing data (also known as communications metadata), intercepts and take-downs; and dealing with red flag incidents. Suggestions are made in each of these areas.

It's recognised that at present and in some circumstances, telecommunications companies could well be infringing the law and/or their operating licences by making certain disclosures. However, it's further recommended that companies and governments work together to increase transparency around: the application of country laws; the public availability of operating licences; the numbers of requests for communications data, communications content, website blocking and network blocking; and occurrence (but not the detail) of the provision of hardware, software and/or services that allow traffic intercept and/or blocking.

Of course any form of intercept or blocking involves a potential human rights infringement. It is therefore important that it is only undertaken when it is protecting others and that the extent of the action is in proportion to the scale of the threat. Governments should resist pressures, internal or otherwise, to go beyond a proportional response.

When calling on companies to establish internal management and accountability processes it is important to focus on the outcomes required. This will allow companies to ensure the right checks and balances are in place without predetermining what might be seen as overly burdensome administrative structures.

It's fully understood that there will be occasions when full disclosures will not be possible. The objective of the proposals made here is to find ways for governments and companies to be more open about their activities without endangering people's well being.

1. THE CONTEXT OF HUMAN RIGHTS AND THE ICT INDUSTRY

1.1 International norms

The conceptual foundation reference for human rights, and its subsequent basis in international law, is the Universal Declaration of Human Rights (UDHR), adopted in its original form by the United Nations General Assembly in 1948.[2] Whilst it is applicable to nation states and not individual companies, a growing number of businesses operating all around the world explicitly recognise the need to build its ethos into their policies. Other critical human rights instruments include the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR).[3] Collectively known as the International Bill of Human Rights, these internationally recognised laws and standards are the basis for the Global Network Initiative Principles and Implementation Guidelines.

During the first five years of the new millennium the United Nations proposed a new set of Human Rights norms that would have placed legally binding obligations on companies. This met significant objections by organisations such as the International Chamber of Commerce (ICC) that led to its abandonment and the appointment of John Ruggie as Special Representative of the UN Secretary-General on Human Rights and Transnational Corporations and Other Business Enterprises. Over a period of several years Ruggie went on to produce "Protect, Respect and Remedy" Framework and set of Guiding Principles on Business and Human Rights that have received widespread approval and were unanimously endorsed by the UN Human Rights Council in 2011.[4]

The last couple of years have seen growing interest from the UN in the application of human rights in an online world.[5] In July 2012 the Human Rights Council adopted a resolution on the promotion, protection and enjoyment of human rights on the Internet. In 2011, the Human Rights Committee approved a new "General Comment" on Article 19 of the ICCPR to give clear guidance on the legitimate restrictions on freedom of expression that a state can make.[6] Important contributions have also been made by the UN Special Rapporteur on Freedom of Opinion and Expression, Frank La Rue. In 2011 he produced a report focused on the Internet and in 2013 a further report on the human rights implications of States' surveillance of communications.[7]

1.2 The telecommunications industry, freedom of expression, privacy and security

Telecommunication companies often find themselves caught between conflicting forces, particularly with respect to crucial UDHR principles covering freedom of expression, privacy and security. As a result they can feel caught between a rock and hard place, having, not only to deal with demands from conflicting stakeholders, but also having to make decisions where legal and other frameworks are far from clear.

2 See https://un.org/en/documents/udhr/

3 See http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx and http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx.

4 "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, available at http://www.business-humanrights.org/Documents/UNGuidingPrinciples.

5 For detailed information on the international human rights frameworks and their relationship with the information and communication technology (ICT) industry the reader is referred to the GNI report Digital Freedoms in International Law

6 Human Rights Committee, "General Comment No. 34: Article 19: Freedoms of opinion and expression," UN Doc CCPR/C/GC/34. 12 September 2011, available at http://www2.ohchr.org/english/bodies/hrc/comments.htm.

7 La Rue, Frank, Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression, Human Rights Council seventeenth session, document A/HRC/17/27 available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf; and Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression, Human Rights Council Twenty-third session, document A/HRC/34/40 available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

1.2.1 An historic perspective

For much of the 20th century phone calls were in analogue form and physically switched across the network in a way that held a continuous circuit from one phone to the other. Most of the time this made it very easy to listen in—requiring little more than a pair of crocodile clips and a set of headphones.

The introduction of low cost, very large-scale integrated circuits in the 1980's and 90's led to a complete transformation of telecommunication networks. At the heart of a modern network everything is digitized into the same binary code used by computers. This eliminates the need for physical switching and ultimately made the Internet possible. In fact the latest telecommunications infrastructure known as next generation networks (NGN) now uses packet switching (a fundamental aspect of the Internet) to route all traffic, including voice calls.

In parallel the last thirty years have also seen the widespread introduction of cellular mobile telephony and, more recently, mobile broadband. Whilst mobile and fixed line telecommunication share the same core network infrastructure, an exclusive mobile approach for the final connection to the customer provides more flexibility and eliminates the need for more expensive connections to individual premises and explains the preferential and rapid take up of mobile phones in emerging economies. For example, in 2011 China Mobile increased their customer base by over 180,000 people per day.

Since the introduction of the telegraph, law enforcement agencies have applied telecommunication technology to investigate crime and catch criminals. In 1910, Dr. Hawley Harvey Crippen was the first criminal to be caught with the aid of wireless communication on steamship passage across the Atlantic. The intercept techniques employed by the police and security services often involve equipment vendors and network operators in their design and implementation. They often use highly sophisticated technology which can be undisclosed for obvious reasons.

Few criticise the legitimate use of ICT in fighting crime and catching genuine criminals. But governments can also abuse the technology. One notable example involved the Azerbaijani regime monitoring SMS votes in the 2009 Eurovision song contest to identify, and subsequently question, people voting for the entry from archrival Armenia.[8]

1.2.2 The role of ICT companies

As attention to the role of ICT companies in facilitating government access to networks grows, some call for telecommunication companies to explain how they deal with inappropriate government actions. Others argue that ICT is morally neutral, that its social impact comes down to how people apply it, and that the purveyors of both the technology hardware and the resultant communication channels, should be immune from any form of accountability concerning their use. In principle companies can challenge governments and even exit countries in protest, but as this report explains, this is not always as easy as it sounds. Whatever the merits of the opposing arguments, when it comes to companies' interaction with governments demanding access to communication traffic data and content, the telecommunications industry carries a significant reputational risk of involvement in human rights abuses committed by those governments.

In response some companies argue that there is no other choice but to comply with government requests and demands if they are to operate in a given jurisdiction. This is true, but it's not to say that there isn't scope for companies to look at the terms of how and under what circumstances they respond to government requests, what company-wide policies and procedures they adopt for handling government relationships, the circumstances and terms under which they enter a market and sign contracts with local partners, and ultimately whether they choose to operate in certain countries at all.

8 BBC News, "Azeri man 'I was picked for Eurovision protest vote'", 21 May 2012, available at http://www.bbc.co.uk/news/uk-18137850.

2. THE OPERATING LANDSCAPE

Fifty years ago, more than 20 per cent of US homes were still without a telephone.[9] For those with a phone, whether in the US or Europe, there was no choice of supplier and just one thing one could do with it – make a call. The fax machine did not yet exist and businesses had to use the telex to send text messages.

2.1 Convergence

Today a telecommunications network connection with broadband capability allows the user, often simultaneously, to: make a call; send a fax; receive an email; order the shopping; access an encyclopaedic knowledge base; download a film; socialise with friends; listen to the radio; catch up missed TV; and bid in auctions. In fact the list is almost endless, as is the list of companies that now provide these services.

WHY CONVERGENCE MATTERS FOR PRIVACY AND FREEDOM OF EXPRESSION

Convergence is creating new ways to communicate and bringing new companies into the market place.

Governments are adapting their legislation and processes to accommodate these changes.

Due to convergence of hardware capabilities we can now do most of these things on our smartphone, our computer, and soon our televisions.

Convergence is also being driven by 'the cloud'. Cloud computing refers to the storage of a user's information in large data centres such that it can be referred to and updated using a multiplicity of devices and software interfaces. Sometimes the processing which would previously have taken place on a personal computer now also takes place on the cloud. The cloud therefore makes it easier for multiple communication platforms such as fixed line and mobile to converge into seamless connectivity.

Just as digital technology has driven the convergence of devices and services, it has also blurred the traditional boundaries of service providers. This means telecommunication operators are often Internet Service Providers (ISPs) and content providers. At the same time traditional content providers have moved in the other direction and are becoming ISPs, and even phone companies. For example, there are a number of companies such as Sipgate, Skype (now owned by Microsoft) and Vonage that offer software that allows phone calls over the public Internet, as well as interconnection with landlines and mobile phones. Google is becoming a vertically integrated company with the acquisition of the mobile arm of Motorola and its recent launch of a broadband Internet network infrastructure using fibre-optics in Kansas City, among other strategic moves.

2.2 Ownership models and liberalisation

In the latter years of the 19th century the telephone was often introduced to local communities by small private businesses. However, as networks grew it was generally decided that telecommunications was a 'natural monopoly' and this led to an international network of mostly government owned, monopoly, fixed line service providers. These are generally known today as the 'incumbents', even though many have now been privatised. Indeed in most of the big telecommunication markets, especially in the developed world, privatisation of the incumbent has been combined with a liberalisation of the market. Subsequent competition has led to a proliferation of service providers, including mobile network operators and some that do not own any of the infrastructure but simply buy capacity from those that do, and re-package it as their own service.

9 U.S. Census Bureau, Housing and Household Economic Statistics Division, available at http://www.census.gov/hhes/www/housing/census/historic/tpgraph.html

WHY OWNERSHIP MODELS MATTER FOR PRIVACY AND FREEDOM OF EXPRESSION

A communications provider independent of government ownership offers an additional human rights checkpoint.

Of crucial interest to this paper is the closeness of the relationship between telecommunication service providers and governments. The following analysis is drawn from the ITU ICT EYE database, which covers 284 fixed line operators across 184 countries and shows that full or partial state ownership is much more likely in less-developed countries.

TABLE 1. LEVELS OF GOVERNMENT OWNERSHIP IN FIXED LINE OPERATORS[10]

Region	State Owned	Part Privatised	Fully Privatised
Africa	41%	43%	16%
Americas	18%	19%	63%
Arab States	35%	46%	19%
Asia Pacific	36%	30%	34%
CIS	23%	31%	46%
Europe	11%	37%	52%
World	26%	33%	41%

Source: ITU Telecommunications/ICT Regulatory 2010 Database, www.itu.int/icteye

As the penetration of phones in developed economy markets has reached near saturation levels and competition has reduced profit margins, many operators have invested in emerging economies to grow their markets.[11] In some cases, this has taken companies into unfamiliar territories where the rule of law can be uncertain, bribery and corruption can be common, the independence of the judiciary may questionable, and government actions can be more opaque than transparent.

As a result it is now not unusual for traditional service providers from the major developed economies to offer service in most countries across the world, including emerging economies. They achieve this either through wholly owned subsidiaries, joint ventures (often with local providers), or by renting in-country capacity. This rapid expansion has increased their risk of being associated with human rights infringements, especially where they have chosen to, or have been required to, partner with government owned operators.

2.3 Regulation, governance and standards

Matters of regulation, governance and technical protocols and standards are essential for the smooth working of the entire communication system. In part this is a technical necessity, so that a call or email originating in one part of the world finds its way to the correct recipient anywhere else on the planet, irrespective of the type of equipment being used.

WHY REGULATIONS AND TECHNICAL STANDARDS MATTER FOR PRIVACY AND FREEDOM OF EXPRESSION

Regulations and standards are also involved in matters of traffic blocking and intercept. For example, there are specific hardware standards for intercept such as the Russian SORM system and the ETSI Legal Intercept Standard covered in section 3.1.4.

The ITU lies at the heart of global telecommunications governance. It was founded in 1865 and is now part of the United Nations. It is the principal global standards setting organisation in the industry and has a membership of 192 countries and some 700 private-sector entities. It is also responsible for allocating global radio spectrum.

In addition to the ITU, there are a wide range of influential standards organisations such as the 3rd Generation Partnership Project (3GPP), the European Telecommunications Standards Institute (ETSI) and other regional members of the ITU's

10 Unfortunately it has not been possible to locate a similar table for mobile. However a lower degree of state ownership would be expected for mobile operators, especially those in liberalised markets.

11 World Bank data compiled by the GSMA shows an average of US $64b per annum private investment in mobile infrastructure across 133 lower income per capita countries.

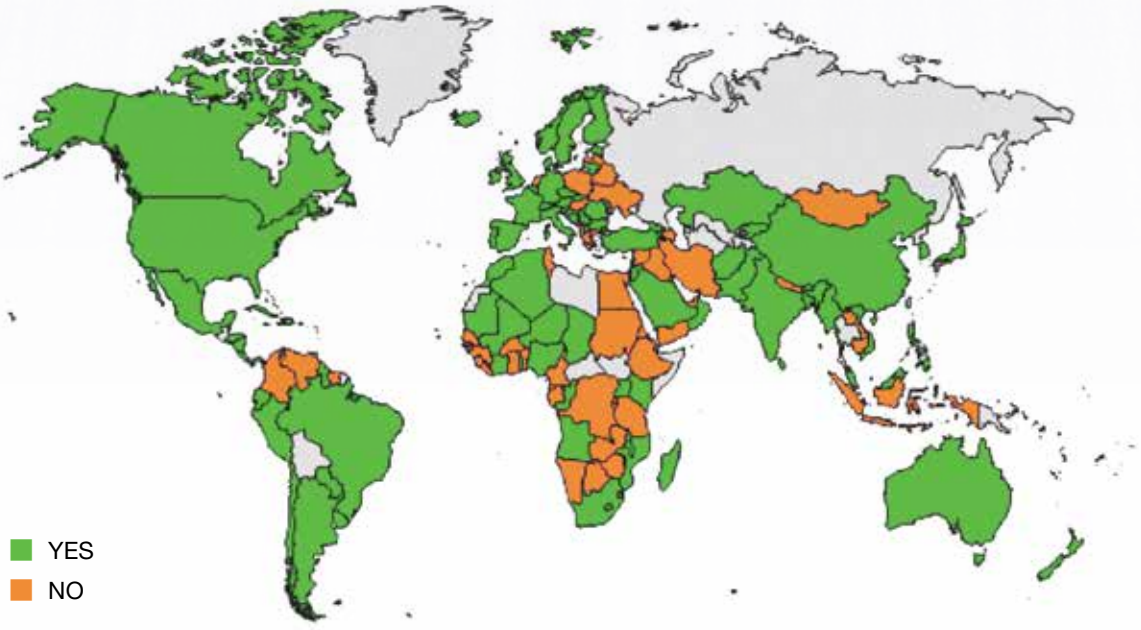
Global Standards Collaboration. On the Internet side there are non-governmental standards bodies including the International Engineering Task Force (IETF) and the World Wide Web Consortium (W3C). Their structure and modes of operation are very different from bodies traditionally concerned with the governance of global telephone networks and they often operate in a far less formal fashion, with a much more diverse stakeholder participation.

Apart from most point-to-point satellite communications, access to the Internet and all other international telecommunications must route through in-country network infrastructure. Such infrastructure is extensive, very capital intensive, and by necessity local in nature. It is therefore far more open to control and regulation by the nation state. The ITU EYE database contains a very extensive list of national legislation pertinent to telecommunications.

Many countries have also introduced a separate telecommunications regulatory authority.[12] The job of the regulator is usually to ensure that the market is fair and open, and that provision of service is equitable and non-discriminatory. It is also important for someone to have control over limited resources such as airwave spectrum allocation, numbering and naming regimes.

Most telecommunication service providers either operate under a general authorisation or have to be awarded, and generally pay for, an operating licence. The authorisations and licences are issued by the government, or via its regulator, and can contain many terms and conditions covering such things as pricing policy, quality of service, fair competition and spectrum allocation. Privacy protection and other matters pertinent to this paper such as compliance with intercept law may also be covered in authorisations and licences. ITU EYE identifies the states that make licensing agreements public and, in some cases, lists where they can be found.

FIGURE 1. COUNTRIES THAT MAKE LICENSING AGREEMENTS PUBLIC



Source: ITU Telecommunications/ICT Regulatory 2010 Database, www.itu.int/icteye

12 See the ICT EYE database for a list of countries with a separate regulatory authority, available at http://www.itu.int/ITU-D/ICTEYE/Default.aspx.

3. GOVERNMENT REQUESTS

The majority of government requests received by telecommunication companies that have the potential to impact privacy or freedom of expression are either to intercept communication traffic or to block it. In either case this can range from a targeted individual or website, through to mass action across the entire network.

FIGURE 2. SUMMARY OF GOVERNMENT INTERVENTION POINTS

	TARGETED	MASS
Switch Off	Discriminate government requests** to 'switch off' specific content. Eg specified web site(s)	Indiscriminate government requests** to switch off entire service channels. Eg suspend services in specific areas.
	Indiscriminate surveillance followed by discriminate filtering and blocking. Eg. Blocking of all SMS messages containing certain words.	
Intercept*	Discriminate government requests** to provide details (usually historic) and /or content (usually real time) of an individual citizen's communications traffic.	Indiscriminate government requests** to undertake or allow an unlimited surveillance of all communications traffic (content and/ or metadata) at certain points in the network.

* Intercept can cover both live intercept of traffic and the recovery of information from stored records.
** In this context 'requests' covers requests and demands.

Most requests lie in one of the four boxes in the 2x2 matrix. The exception concerns filtering and blocking which is a combination of mass surveillance followed by targeted switch off and is covered by the central box.

The following two sections cover privacy (primarily impacted through intercept) and freedom of expression (primarily impacted through blocking). Relevant legislation from the European Union, Russia, Sweden and the United Kingdom is described here in order to illustrate the types of regulatory frameworks in which telecommunication companies often operate.

3.1 Privacy

In general, telecommunication customer and user information would be expected to be confidential. Exceptions are, however, allowed in limited cases. Both aspects are recognised in separate clauses of Article 37 of the ITU Constitution. In the European Union, the e-Privacy Directive requires member states to ensure through national legislation the confidentiality of communications (i.e. content) and related traffic data. Two exceptions are permitted. The first is to safeguard national security and to ensure the investigation of criminal offences, provided this is a necessary, appropriate and proportionate measure. The second is to allow the delivery of the service; maintain its security (e.g. virus protection); and minimise congestion.

This report focuses on activities that take place with the knowledge, but not necessarily the concurrence, of the network operators. There may, of course, be an additional set of covert, unauthorised surveillance activities undertaken by state authorities when the fact that an intercept point even exists is unknown to the operator.

3.1.1 Information flows

Telecommunication operators need to keep information for billing purposes – numbers dialled, length of call, etc. The mobile network also needs to know where users are located in order to effect a connection, and operators retain that information for billing purposes and sometimes dispute resolution. It is also important to make sure that Internet traffic is properly managed and protected from malicious software such as viruses and other hostilities such as denial of service attacks.

Whether the communication is a voice call routed over the public switched telephone network (PSTN) or Internet traffic, there are essentially two levels of information. The first level is information (metadata) that controls and manages the routing.

The second level is content. In the case of PSTN voice calls the content refers to what is being said, and the control information will typically cover:

- number dialled;
- number to which the call is routed;
- date and time of start and end of communication; and,
- in the case of mobile phones, the cell location(s).

In the case of Internet communications, large amounts of transmitted data will be broken up into more manageable chunks known as 'packets'. Each packet contains a header containing control information and a payload containing the content. Critical components of a header include:

- source IP address;
- destination IP address;
- information determining the required quality of service, protocol type, etc. This information can indicate the type of data being carried.

The header contains all the information an ISP needs to enable the communication. If the ISP (or anyone else) inspects the payload (i.e. the content) for reasons other than its intended purpose or audience, then this is termed Deep Packet Inspection (DPI).[13]

Note how the inherent flexibility of the Internet is creating a further blurring of traditional technical boundaries – for example with the advent of Voice over Internet Protocol (VOIP) phone calls.

3.1.2 Intercept by and for government agencies

A primary purpose of the state is to ensure the safety and well being of its citizens and its economy, and it is for exactly this reason that governments around the world approve laws allowing them to intercept telecommunication traffic in line with the ITU Constitution. In practice there are essentially three levels of surveillance:

1. Access to historical routing and traffic data for a particular individual.
2. Live intercept of the content of a communication for a targeted individual.
3. Mass surveillance of all traffic.

In order to understand the roles of the main actors it's important to cover three factors: the technology involved; the legal context for each country of operation; and the extent to which the government has direct access or is dependent on the service provider to allow access.

Sections 3.1.3 and 3.1.4 cover traffic internal to a country. Cross-border traffic is covered in section 3.1.5.

3.1.3 Routing and traffic data (communications metadata)

The Data Retention Directive requires EU member states to adopt measures ensuring the retention of communication data for the investigation, detection and prosecution of 'serious crime'.[14] Data must be retained for a period of not less than six months and not more than two years. The list of data to be retained seeks to allow the tracing and identification of the source and destination of a communication, the date, time and duration of a communication, the type of communication and the equipment used for the communication and its location.

Current UK legislation permits access to routing and traffic data by a wide range of public officials including the police, intelligence services, tax and customs authorities, and other public authorities designated in secondary legislation.[15] The term 'serious crime' is not defined in the EU directive and privacy campaigners are concerned that the wide range of government employees with access permission in the UK goes too far.

In Sweden government access is tighter than the UK and restricted to law enforcement agencies, and even then only permitted in cases involving suspicion of serious crime of the type that could lead to imprisonment.[16]

13 See the technical glossary for more information on DPI

14 Data Retention (EC Directive) Regulations 2009

15 Regulation of Investigatory Powers Act 2000 (RIPA)

16 Swedish traffic data retention is covered by the Law on Electronic Communications (2003:389, as amended with entry into force on May 1, 2012) and the Code of Judicial Procedure (1942 :740)

In Russia access to data is provided to those public authorities ensuring national security and safety, and the detection and investigation of criminal offences.[17]

In Sweden and the UK, the state authority applies to the service provider who responds with the requested routing and traffic information. In Russia state authorities have independent and direct access to operators' databases.

In Sweden the application must be made by the police, security service or a government office, and approved by a prosecutor, with court approval or in cases of investigation and inquiry by the police or the customs with a notification to The Swedish Commission on Security and Integrity Protection. No court order is required in any of the other countries.

3.1.4 Targeted intercept

In most countries, interception by or on behalf of government departments of the *content* of user communications is generally more tightly controlled than access to traffic data.

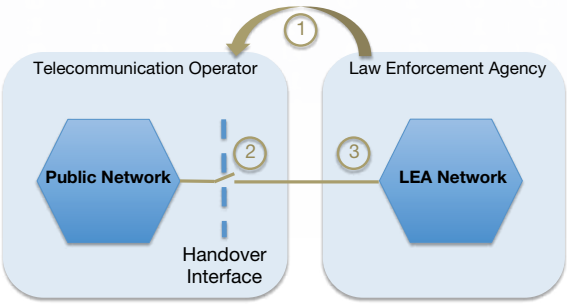
In the UK requests for intercept warrants must be made by very senior officials such as the Director General of the Security Service or a Police Chief Constable, and require approval from the Secretary of State.[18] They must relate to a matter of national security, or for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well being of the UK.

A similar situation exists in Sweden where the application must be made by the police, security service or a government office, and approved by a prosecutor, with court approval.

In Russia, the head of any public authority responsible for the detection or investigation of criminal offences or ensuring public security or safety should apply for a court decision/permission to intercept communications.[19] However, the operators of communication networks are also obliged to provide technical and other access to their networks, which could allow government agents to enact an intercept without presenting the warrant to the network operator.[20] Allegedly, this is made all the more possible as network service providers operating in Russia often have government officials based in their premises to effect direct access.[21]

Targeted intercept, also commonly referred to as 'legal intercept', is well documented under international standards.[22] It is a fundamental premise of these standards that the service provider maintains responsibility for delivering secure private communications for its customers. To ensure this happens the network architecture should be designed such that there is a distinct separation between the Public Network and the Law Enforcement Agency (LEA) Network. There are then standardized interfaces that manage the hand-over of data between both networks. According to the standard the interface should be managed by the network operator who allows the intercept on receipt of an official warrant.

FIGURE 3. ETSI LEGAL INTERCEPT STANDARD



1. LEA supplies warrant to telecom operator.
2. Telecom operator provides access to approved circuit.
3. LEA accesses designated communication traffic.

17 Russian data retention is covered by the Communication Law, and Degrees No 87 and No 538.

18 UK targeted intercept is covered by the Regulation of Investigatory Powers Act 2000 (RIPA) (section 8(1)).

19 Article 63, p. 1 of Communication Law of Russian Fed. of July 7, 2003. Article 63, p.3 of Communication Law and Law on Conducting Activities to Ensure National Security and Defence and Public Safety of Russian Federation of Aug 12, 1995. Article 64, p.2 of Communication Law. Degree No 538 of Federal Government of Aug. 27, 2005. Degree No. 87 of federal Government of Feb 18, 2005.

20 Article 64, p.2 of the Communication Law

21 In a number of countries the telecommunication company engineer enabling the PN/LEA connection has to be a citizen of that country. In cases where the network operator is headquartered overseas, the engineer is not allowed to reveal the detail of his activities to his/her overseas superiors.

22 See http://www.etsi.org/website/technologies/lawfulinterception.aspx

Country administrations may require different levels of interception capability. A typical requirement may be for a maximum capacity of 1 in 10,000. That is to say the system would be capable of simultaneously intercepting a maximum of 1 in 10,000 lines. Some countries require significantly higher intercept capabilities.

It should also be noted that whilst a country's legislation may require an official warrant to authorise an intercept, this does not necessarily mean that the hand-over takes place according to the ETSI standard. In other words, if the LEA has direct system access then that access will not have to be enabled by the network operator even though the need for an official warrant is still mandatory.

3.1.5 Mass intercept

Whereas 'targeted intercept' involves tapping into a specific person's connection, 'mass intercept' describes a situation where all traffic has the potential to be monitored continuously. Technically this requires the network operator to provide unrestricted access to all the communication activity occurring at a specific point on the network. In many countries mass surveillance is generally the domain of state security and secret service agencies and the technology deployed is often a closely guarded secret.

Once the connection has been made, little if any further intervention is required from the telecommunication company and the government agencies will effectively be able to scrutinise all the data being transmitted. This may require de-multiplexing of data channels and, in some cases, decryption.

In Sweden the so-called 'FRA Law' allows all cross border communications to be monitored by the FRA (the National Defence Radio Establishment).[23] The law stipulates that the FRA needs to apply for specific permissions from a special court for Defence Intelligence, "Försvarsunderrättelsedomstolen", and the FRA may only search the intercepted communications using pre-approved search terms. The search terms are defined by the FRA, in accordance with approved areas such as 'foreign threats' and 'foreign affairs' and must be approved (on a general level) by the cabinet or by government authorities such as the ministry of defence or military intelligence. In practice, some Swedish intra-country communication can also be monitored since it often crosses borders at some point. However, such communications should be destroyed if they are intercepted.

UK law provides for a warrant to be issued by the Secretary of State allowing the intercept of all external communications, i.e. communications that travel across the UK border.[24] However, although the UK government states that all such activity is legal, neither the existence of the warrant, nor its content is publicly acknowledged.

The law in Russia makes little, if any, distinction between targeted and mass intercept and the provisions already described in section 3.1.4 apply.

In recent releases concerning their own operations Tele2 have disclosed a number of countries where the authorities have direct access to their networks.[25] These include the Baltic States, Croatia and Kazakhstan. In these cases no warrant is supplied and no intervention is needed by Tele2 to allow the intercept to take place. In fact Tele2 state that in such cases they have no way of knowing when an intercept has occurred.

3.2 Freedom of expression

Restricting or blocking a person's access to communications is often seen as a curtailment of the human right to freedom of expression. Blocking can be imposed for a number of reasons, some politically motivated (such as reasons of state security), some commercially motivated (such as access to copyrighted material) and some morally motivated (such as access to child pornography). In any case the rationale is often linked to criminal or civil law.

3.2.1 Targeted blocking

Targeted blocking generally involves blocking access to certain websites. This can either be achieved by asking the organisation hosting the website to take it down, or by preventing completion of the access

23 Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signals intelligence in Defence Intelligence)

24 Regulation of Investigatory Powers Act 2000 (RIPA) (section 8(4))

25 See https://www.youtube.com/watch?v=etGNp1Ttio0 and https://www.youtube.com/watch?v=QX3RsDgBtXw

request in some way. The former is not the focus of this paper as it is more relevant to content providers.

There are essentially two junctures at which an ISP can block access to a given website.

The first would be to stop the request for access from reaching the website:

> When a user types a url such as www.bbc.co.uk into their browser, the url has to be converted to a numeric IP address (e.g. 212.58.246.94) using the domain name system (DNS). If the url is not found on a local DNS server then a search will be made on servers across the Internet with more complete databases. Once the numeric IP address has been identified this is sent to an ISP router that will look up the numeric IP address in its routing table. If it is a commonly used IP address then it's likely to be in the routing table of the first router encountered (the edge router). If it's not available at the edge router, then the packet will be sent down a default routing path to the ISP's peering router on the Internet backbone until the address is resolved and the packet eventually sent on its way.
>
> If the ISP wishes to block the access request reaching the website then one way is to remove the url from their DNS server. This is only partially effective as it is relatively simple to configure a computer to use an alternative DNS server. Another way is to examine the IP address against a list of 'blocked' websites and prevent the packet from going any further. Many routers on the market have this capability.

The second would be to allow the request to route through to the website but then prevent the returning content reaching the user:

> In this case the point of origination of packets coming into the ISP network is examined against a list of 'blocked' websites and if there is a match the packets get diverted somewhere else such as in Internet 'black hole'. Again this is standard capability for many routers.

Although the UK has no general legislation governing website blocking, ISPs have received a number of specific High Court Orders requiring them to block certain file sharing websites because of extensive copyright infringement. There is also a voluntary agreement between the UK government and ISPs that websites containing child pornography that has been declared illegal by an independent organisation, the Internet Watch Foundation (IWF), will be blocked. In this case ISPs receive a list supplied by the IWF over a secure interface. The ISPs do not have direct access to the list and are obliged to keep it confidential and secure.

As in the UK, Sweden has no general legislation governing website blocking, although like the UK there is a voluntary agreement for ISPs to block websites containing child pornography.

In Russia, the Law on Mass Information and the Law on Protecting Children from Information Harmful to their Health and Development require ISPs to block sites containing a very wide range of issues including: pornography; gambling; information that is considered harmful for the health and/or development of children; content that denies family values and encourages disrespect for parents and/or other members of the family; justifications of illegal behaviour; foul language; information constituting a state, or other, secret protected by law; as well as websites with appeals to, or justifications for, terrorism or the distribution of extremist materials. Blacklisted websites that haven't been taken down are contained in an on-line registry[26] introduced under Federal Decree 1101. A number of agencies can order the blocking of a site including the Federal Authority Supervising Traffic of Narcotics, the Federal Authority on Consumer Protection and Human Rights and the Federal Supervisor of Communications, IT and Mass Media (NRA).

The ultimate sanction is to disconnect an Internet user from access altogether. EU law states that Internet access cannot be restricted if it impacts on the fundamental rights of users, except if taken following a fair and impartial procedure. In Sweden no provisions exist to do it, however in the UK, the Digital Economy Act 2010 has a provision that would require ISPs to cut off persistent downloaders

26 See http://zapret-info.gov.ru/

of copyrighted material. There has been prolonged objection to this provision by UK ISPs and free expression advocates, often quoting the EU legislation. At the time of writing there was no expectation that this provision of the Act would be enacted before 2014 at the earliest, if at all.

In Russia the disconnection of an individual's Internet access is considered to be covered by legislation enabling the closure or interruption of a complete communication service (as described in section 3.2.2). It can be enacted by any public authority authorised to conduct activities to ensure national security and defence, or detection and investigation of criminal offences. Grounds for disconnection can include:

- evidence about preparation or commission of a wrongful act for which a preliminary investigation is required;
- information received about people who are preparing to commit, or have committed, a wrongful act for which a preliminary investigation is required;
- possibility of serious crime; and
- threats to state, military, economic or ecological security of the Russian Federation.

3.2.2 Mass blocking

Whereas targeted blocking applies to specific users or websites, mass blocking relates to the disconnection of whole sections of a network. Governments may seek to do this at times of national emergency and often have made the legal provisions well in advance.

The EU Authorisation Directive allows for the suspension of normal communications service during major disasters or national emergencies to ensure communications between emergency services and authorities. The EU also recognises that nation states can legislate in order to suspend or interrupt a telecom service.[27]

In the UK the police Gold Commander, the officer in highest authority during a major incident, can ask network providers to supply privileged access for emergency service phones.[28] In addition, the Secretary of State can order the industry regulator to suspend specific networks, services and facilities, to take effect as soon as the network operator is notified, and for an indefinite period of time.[29] Networks can be closed down in the case of a threat to public safety and public health, or in the interest of national security.

In Sweden the telecommunication law does not foresee an occasion when an electronic communications service could be suspended outside of the case where the operator itself breaches some of the provisions of the law and where this constitutes a serious threat to public order, public security, or public health, or if there are serious financial or operational problems.

The Communications Law of the Russian Federation includes an obligation to ensure "technical and other means" to close or suspend services if and when requested by security authorities. The Law on Conducting Activities to Ensure National Security and Defence and Public Safety also allows public authorities ensuring national security, defence and public safety, to close or suspend communication services. In the latter case this law states that the closure of communication services is allowed only in case of a direct threat to the life or health of persons, or in the case of a threat to the national security or threat to the economical or ecological situation of the Russian Federation.

27 Recital 7 of the Framework Directive.
28 Under the Civil Contingencies Act 2004.
29 Under the Communications Act 2003.

4. THE MORAL MAZE

Compliance with the law is generally seen as the minimum standard of corporate behaviour. To many though, companies are expected to go beyond the legal minimum and take proactive action to contribute to society and the environment – a concept embraced by the notion of 'corporate responsibility'. When companies fall short of such societal expectations then democratic societies turn to governments to use their legislative powers to set enhanced minimum standards. But what happens when governments themselves circumvent international law, or even their own national law?

Finding the right path through the moral maze of human rights impacts arising from the interaction between telecommunications companies and governments can be a tricky exercise. The report now examines some of the pitfalls and possible solutions.

4.1 The interdependent and interrelated nature of human rights

Enshrined in international human rights standards is the notion that all rights are indivisible, interdependent and interrelated – and that the improvement of one right facilitates the advancement of others. Yet there can be times when clear tensions exist between the protection of privacy, freedom of expression and personal security.

In the case of state action, international human rights law recognises that there will be limited occasions such as "times of war or other public emergency threatening the life of the nation" when the usual protection to freedom of expression and freedom of information and privacy can be suspended.[30]

When these tensions arise, a telecommunications company can find itself in a position of having to take decisions with implications for individual rights with conflicting stakeholder views, or conflicting interpretations of the law, or even, of being required by state officials to circumvent the law. The latter situation is made all the more difficult when such requirements are made by those whose job it is to uphold the law.

The next section considers some of the measures that can help companies navigate the right path through this moral maze.

4.2 Choosing the right path

The first step in selecting the right path is to recognise the warning signs. The second step is to respond appropriately.

The starting point for any company should be the specific application of international human rights frameworks to the telecommunication sector. Next will be a review of the relevant legislation in the proposed country of operation. This report has only looked in detail at one regional set of legislation (the EU) and three specific countries (Russia, Sweden and the UK). Although this is a limited set, it is interesting to note the similarity of basic legislation that allows the state to intercept and block traffic. For example, all three require a warrant (or similar) for targeted and mass intercept. The UK and Russia allow the government to switch off networks at times of emergency, although this possibility is apparently not foreseen in Sweden apart from time of war.

However, there are differences in the detail of the legislation and in its implementation that can indicate levels of risk exposure for a telecommunications company. Important issues to consider are:

1. **Transparency – is the state clear about what actions it can legitimately undertake? Are there a laws or regulations in place regarding interception and blocking of communications?**

   Take, for example, the three countries studied for this report and consider transparency around mass intercept. This varies significantly as described in section 3.1.5. Sweden has a specific law that describes permitted activities and safeguards. Mass intercept in the UK is

30 For example see Article 15(1), European Convention on Human Rights.

covered by a legal clause, but there is very limited information about its implementation. In Russia it is not entirely clear if a warrant is required as in the UK, or if the legal obligation to install necessary equipment makes the need for a warrant redundant.

Additional to government stipulations enabled through legislation are any supplementary requirements placed on telecommunication operators through licencing/authorisation arrangements.

2. **Rights of Appeal – do telecommunication companies have a right to appeal against state interventions?**

   The legislation of all three countries studied here provide some routes to appeal against requests for intercept and blocking. Whilst this may be in place, it is also important to recognise that governments will often expect an immediate response and that in such cases appeals will take place after the intervention. Although this may make the appeal process appear somewhat academic it is still good practice for the legislation to include such checks and balances.

3. **Accountability – does the state publish statistics regarding its use of intercept and blocking?**

   Much of what happens in the world of intercept remains under wraps, especially with respect to the technology adopted. In the UK, information obtained using intercept techniques is often not presented in court simply because that would involve having to disclose the methods adopted in obtaining it. However, there are opportunities to aggregate statistics to enable the disclosure of information such as the number and types of intercept, as well as communication blocks.

   The US, for example, publishes the number of targeted intercept (wire tap) warrants issued.[31] The UK also publishes this data[32] along with the number of applications for routing and traffic data (communication traffic authorisations). This information is included in the Annual Report of the Interception of Communications Commissioner, which in 2011 disclosed 2911 lawful intercept warrants and 494,078 communications data requests.[33] The Commissioner also reports extensively on his investigations to ensure that all authorities, including the intelligence agencies, are acting lawfully. Sweden publishes similar information, however this does not include lawful interceptions conducted by the secret police, and reported that the number of intercepted and monitored persons increased by 17 percent to 2,040 people in 2011 compared to 1,744 in 2010.[34]

4. **Behaviour – is there evidence, anecdotal or otherwise, that gives cause for concern?**

   There is certainly anecdotal evidence that some governments have found ways of circumventing the spirit of their own legislation. This is particularly the case where governments have their own officials based in the network operators facilities or have required equipment to be installed that gives them direct and unfettered access to system data and traffic without the need for the official operator's intervention. Such access is not consistent with the protocols defined in the international standards on legal intercept.

Assuming that a telecommunication company has undertaken this basic level of risk assessment and has followed many of the due diligence steps described in the GNI Principles and Inplementation Guidelines and other guidance, how should it then respond? At a binary level a telecommunication

31 Available at www.uscourts.gov/Statistics/WiretapReports/WiretapReport2011.aspx

32 See http://www.intelligencecommissioners.com/docs/0496.pdf

33 This is broken down into 52% subscriber data, 25% traffic data, 17% combined data, 6% service data.

34 See http://www.aklagare.se/PageFiles/7273/Rapport%20till%20regeringen_tvangsmedel.pdf and http://www.riksdagen.se/sv/Dokument-Lagar/Forslag/Propositioner-och-skrivelser/Hemlig-teleavlyssning-hemlig-_H00347/?text=true (Government report to Parliament, in Swedish).

company could choose not to operate, or sell equipment, in high-risk countries well known to infringe human rights. This might work in a small number of cases but such an approach is complicated by a number of factors:

- ICT infrastructure often helps citizens campaign for democracy and their rights, so self-imposed exclusion from a country may not be a net human rights positive;
- withdrawal may increase the risk of human rights infringements if user choice is then exclusively limited to government controlled operators;
- a company presence in the country should be an opportunity for constructive engagement on human rights – either bilaterally or through an industry grouping;
- regimes change and, once in a country, the very large capital investments involved and many employees on the ground mean it is not easy for telecommunications operators to exit quickly;
- the infrastructure as such will remain in the country; and
- infringements are by no means the exclusive domain of extreme, un-elected, authoritarian governments.

When deciding whether to challenge a government demand, companies must consider the safety of their own employees working on the ground in the country, which could be jeopardized in retaliations. A reluctance to challenge may also arise from a desire to protect commercial interests, including the continuation of operating licences, and also a desire not to damage relationships with the government as a major customer.

When considering the opportunity for companies to review and challenge government requests it is also important to recognise the very large number of requests received for communications metadata, as well as intercepts, and the practicalities of detailed scrutiny. In addition, the operator will often not know the reasons behind a particular request.

On 1 April 2012 US Congressman Edward Markey wrote to nine mobile operators, including AT&T, Sprint and Verizon, requesting information on US law enforcement requests for subscriber information.[35] He subsequently reported that in 2011 law enforcement agencies made more than 1.3 million requests of wireless carriers for the cell phone records of consumers. Only T-Mobile (owned by Deutsche Telecom) declined to provide the requested data to Mr Markey.

In a recent, and very rare case in the USA an unidentified telecommunication operator challenged the government's use of a National Security Letter to obtain access to customer records without a court order.[36] In response the U.S. Department of Justice filed a civil complaint claiming that the company, by not handing over its files, was interfering "with the United States' sovereign interests" in national security. Very few details of the case have been released on security grounds, but on March 13, 2013 a federal court judge ruled that the 'gag order' component of the NSL was unconstitutional.[37]

It is also important to recognise that for a large number of telecommunication operators (see Table 1) the government holds a major equity interest.

Whilst voluntary exclusion from a given country is inevitably going to be rare, there are a number of procedural actions companies can take. In this respect there is plenty of guidance available including: the GNI Principles; the UN Guiding Principles on Business and Human Rights; the Access Telco Action Plan; the Telecommunications Industry Dialogue on Freedom of Expression and Privacy Guiding Principles; and the European Commission Guidance on the ICT sector and the Ruggie Principles.[38] It is recommended that

35 Available at Available at http://markey.house.gov/press-release/democratic-members-call-hearing-cellphone-tracking-law-enforcement-officials.

36 See Jennifer Valentino-Devries, "FBI Secret Letters Face Rare Challenge," *Wall Street Journal*, 17 July 2012, available at http://professional.wsj.com/article/SB10001424052702303567704577519213906388708.html. NSLs are similar to the arrangement in Russia and the UK described in this report.

37 Matt Zimmerman, "In-Depth: The District Court's Remarkable Order Striking Down the NSL Statute," EFF, 18 March 2013, available at https://www.eff.org/deeplinks/2013/03/depth-judge-illstons-remarkable-order-striking-down-nsl-statute.

38 Expected to be published in June 2013

companies should establish a set of written processes covering their own actions and, where relevant, their suppliers, when:

1. **Bidding for a new, or renewal of an existing, operating licence**

   In such instances companies should explicitly state in their bid their corporate position and process for handling government requests for traffic or routing data, intercepts and take-downs. It may also be appropriate to state the company's position on bribery and corruption.

   Whilst this action would represent best practice at all times, it is particularly crucial when bidding for licences when the regulatory regime has not been properly delineated.[39]

2. **Handling requests for communications metadata, intercepts, and take-downs**

   Whenever possible companies should ensure requests are both legal and have originated from pre-agreed legitimate sources.

   Given the very large numbers of requests that may be made, and the fact that the reason behind requests is often not known, companies should also establish a set of human rights red flag triggers. For example, this might include: a sudden proliferation of requests around an election or other politically sensitive event; or requests for extensive action without any clear reason; or requests that cause unnecessary service disruption and could be more tightly focussed or better timed.

3. **Dealing with red flags**

   When a red flag is triggered then there should be a pre-defined process to follow, with fast-acting escalation to the most senior levels of the company if there is a very high risk of large-scale human rights abuse.

   It should also be recognised that sometimes speed of action is necessary to protect life (e.g. if bombs are being triggered over the network). The processes will need to accommodate such instances.

   In some circumstances it may also be helpful to call on other governments to intervene through diplomatic channels.

39 For example, see the case of Burma. Human Rights Watch, "Reforming Telecommunications in Burma," available at http://www.hrw.org/reports/2013/05/19/reforming-telecommunications-burma.

5. THE IMPORTANCE OF TRANSPARENCY

In the ICT industry, when it comes to government interventions affecting citizen privacy and freedom of expression, Google led the way with its 'Transparency Report' indexed by country.[40] Google's report provides:

- a breakdown of day by day traffic data for each of their services;
- a six monthly report on any government 'take down requests' and Google's response; and
- a six monthly report on the number of government requests for user data, the percentage fully or partially complied with and the number of users/accounts specified.

Many multinational telecommunication companies publish sustainability reports, with some reporting on their general policies around intercept and blocking, though none provide the level of detail in the Google Transparency Report. It's also important to recognise that there will be occasions when full disclosures will not be possible. For example, telecommunications companies could well be infringing the law and/or their operating licences by disclosing certain information. However, as the Markey investigation in the USA demonstrates, some quantified information can be released without endangering national security.

Telecommunications companies seeking to demonstrate credible interest in and concern for the human rights impact of their businesses have an opportunity to work with governments and other stakeholders to discuss how both parties might increase transparency around the volume of requests made and complied with. Some ideas are detailed below that could form the basis of the discussions. In the case of government disclosures and transparency there are already some good examples to draw on such as the FRA law in Sweden and the Interception of Communications Commissioner's report in the UK as highlighted in section 4.2.

5.1 Transparency and service provision

For each country of operation, it's recommended that both network operators *and* governments consider the following disclosure areas:

1. The country's laws that apply to the blocking and intercept of communication traffic, covering both targeted and mass interventions; and, in the case of companies, how they interpret the law.
2. Whether operating licences are publicly available and if so where they are located.
3. The number of government requests for communications metadata.
4. Whether government agencies have direct access to telecommunication company communications metadata using electronic means or via government agents having open access to company facilities
5. The number of government requests to intercept communications content under a legal intercept arrangement.
6. Whether parallel traffic feeds exist from the telecommunication network to one or more government agencies allowing the government unlimited access to monitor either intra-country communications or inter-country communications.
7. The number of government requests to block access to websites with a top-level breakdown of the reasons.

40 The Electronic Frontier Foundation publishes an annual assessment of a small selection of US companies including ISPs, telecommunications operators, mobile services, cloud storage services, and web companies available at https://www.eff.org/pages/who-has-your-back/#transparency. Other companies that have started to publish transparency reports in include Dropbox, Leaseweb, LinkedIn, Microsoft, SilentCircle, Sonic.net, SpiderOak, and Twitter.

8. The number of government requests to close down any part of the in-country network with details of the incidents.

9. Disclosure of any government requests to transmit specific messages to the users of network services without the message identifying it is from the government.

5.2 Transparency and telecommunications equipment

For each country of operation, it's recommended that both network equipment vendors *and* governments consider the following disclosure areas in a given timeframe:

1. Whether hardware that allows traffic intercept has been installed.

2. Whether software that allows traffic intercept has been installed.

3. Whether support services such as consultancy or training in relation to traffic intercept have been supplied.

4. Where any of 1, 2 or 3 is relevant then describe the country's laws that apply to the intercept of communication traffic, covering both targeted and mass interventions.

5. Whether hardware that allows website blocking has been installed.

6. Whether software that allows website blocking has been installed.

7. Whether support services such as consultancy or training in relation to website blocking have been supplied.

8. Where any of 5, 6 or 7 is relevant, then list the country's laws that apply to the blocking of communication traffic, covering both targeted and mass interventions.

6. NEXT STEPS

Mass access to instantaneous multi-media communication often exposes human rights abuses to the world as they happen. We see evidence of this pretty much every day and once recorded in digital format, the data can now be held and accessed indefinitely with the ease of a few mouse clicks. In a world made more transparent by ICT it seems almost inevitable that there will be pressure on both governments and companies to be more open in the future.

In the meantime technology will not stand still and further human rights challenges will present themselves. For example, we are now entering the age of 'big data'. Our use of digital technologies to communicate and run our lives, our homes, our purchases, and our travel, among other activities, leaves a significant digital trail. Not only can this trail be interpreted to discover what we have been doing but, by comparing one person's trail against general behaviour patterns, it might be possible to predict what we might do next with some level of statistical accuracy.

Any form of intercept and blocking involves a potential human rights infringement. It is therefore important that it is only undertaken when it is protecting others and that the extent of the action is in proportion to the scale of the threat. It should also only take place in a clear and transparent legal framework that has well defined opportunities for challenge and requirements for accountability. Governments should resist pressures, internal or otherwise, to go beyond a proportional response.

When calling on companies to establish internal management and accountability processes it is important to focus on the outcomes required. This will allow companies to ensure the right checks and balances are in place without predetermining what might be seen as overly burdensome administrative structures.

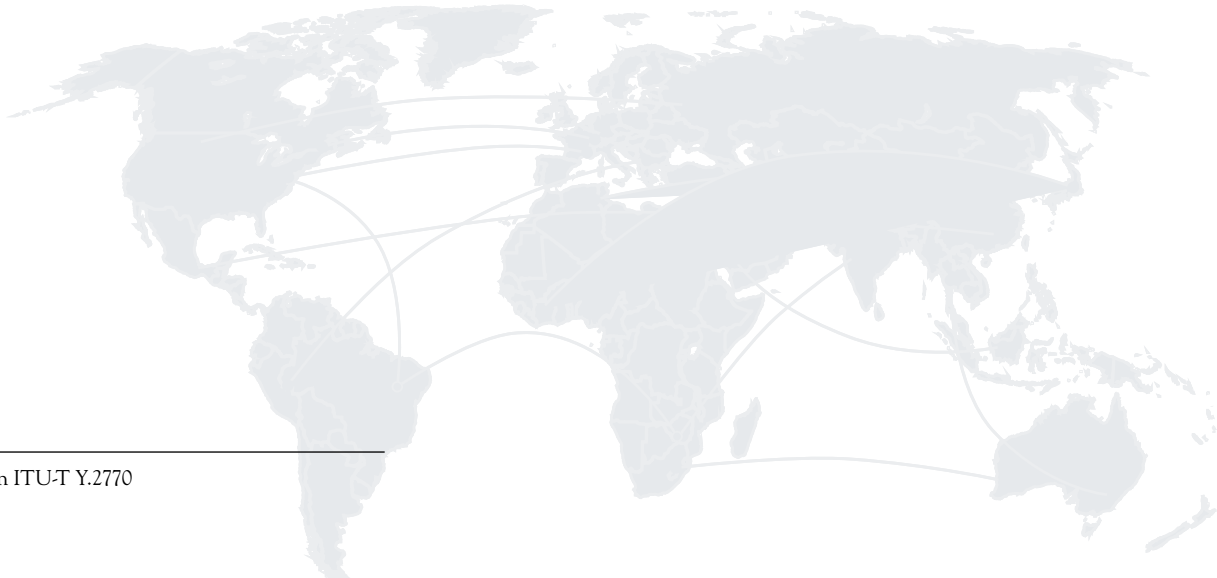
The specific proposals made in the previous section are intended for consideration by both industry and governments. It is recommended that industry and governments develop these as a collaborative process involving external stakeholders.

One area not considered in this report but certainly worthy of further investigation is that of cost allocation. Whether it is the provision of information, the blocking of content or the installation of intercept hardware, there will be a cost incurred. Governments may consider that the telecommunication companies should absorb this as part of their licence to operate. However, if the government is billed for a service provided then this may deter unnecessary requests and demands. In the dialogues that will now hopefully ensue, consideration should also be given to transparency around how these costs are allocated.

Whilst this is inevitably an area where total transparency is often counter to the wider interests of society, there is an opportunity for both parties to become more open about their activities without endangering people's well being. Indeed, when companies come from countries with governments that both advocate the principles of human rights and are trying to influence other regimes less respectful to this agenda, then it's important that the companies can point to best practice in terms of government regulation, performance and transparency in their home market.

ANNEX 1. TECHNICAL GLOSSARY

Address	A digital code identifying a virtual location.
Deep Packet Inspection (DPI)	Inspecting the payload (i.e. content) of a packet. There are various working interpretations of DPI including a specific definition from the ITU.[41]
Domain Name System (DNS)	The system that converts character based web addresses (URLs) into numeric IP addresses.
Internet Protocol (IP)	The internet has a large suite of protocols for transmitting and receiving different types of packets.
Metadata	This term is used to refer to 'data about data'. Routing and traffic data for a communication (including source, destination, timing, etc., but excluding the content of the communication) is a form of metadata.
Multiplexing	Technique allowing multiple communication channels to be transmitted down a single cable.
Next Generation Networks (NGN)	Often replacing multiple switched networks, NGNs convert traffic to internet packets allowing all traffic to be carried on a single platform.
Packets	Internet traffic is cut up into smaller packets of information that are recombined in the right order at the receiving end. A packet comprises a header (for traffic management) and a payload (the content).
Protocol	The format and rules for communicating data.
Router	A device that interrogates a packet's header and routes it along its correct pathway towards its intended destination.
System of Operative Search Measures (SORM)	Specific interception hardware mandated in Russia and other former Soviet states.
URL	Uniform Resource Locator. The web address in character form such as **www.itu.int**.



41 Recommendation ITU-T Y.2770

Global Network Initiative

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. To learn more, visit: **www.globalnetworkinitiative.org**.