Human Rights Challenges for Telecommunications Vendors: Addressing the Possible Misuse of Telecommunications Systems

Case Study: Ericsson

Case Study Number 2

NOVEMBER 2014

Institute for
Human Rights and Business

Shaping Policy ▪ Advancing Practice ▪ Strengthening Accountability

Case Study Number 2

NOVEMBER 2014

Human Rights Challenges for Telecommunications Vendors: Addressing the Possible Misuse of Telecommunications Systems

Case Study: Ericsson

About the Digital Dangers Project

"Digital Dangers: Identifying and Mitigating Threats in the Digital Realm" is a project developed by IHRB in collaboration with the School of Law at the University of Washington in Seattle. The project builds on IHRB's involvement in the European Commission ICT Sector Guide on Implementing the Guiding Principles on Business and Human Rights[1]. Digital Dangers identifies a number of areas including security, safety, free assembly, free expression and privacy where ICT companies and other actors would benefit from more in-depth analysis and policy oriented recommendations.

The aim of the Digital Dangers project is to encourage companies to be open and transparent about the complex dilemmas they face in respecting freedom of expression and privacy by sharing their experiences to spark debate with governments and civil society and bring about positive change.

The Digital Dangers methodology is unique. Once a specific topic and company have been selected as the subject of a Digital Dangers case study, an IHRB researcher is "embedded" into company operations, with permission, for a short period of time to observe dilemmas and complexities first hand. The company which is the subject of the case study is able to review IHRB's report before publication, but IHRB maintains full editorial control. IHRB does not accept funding from companies for these case studies; their value lies in their independence and impartiality.

In addition to the case study series, an online global database is also being developed as part of the Digital Dangers project. The completed database will be publicly available and highlight examples of where human rights may be infringed in the digital world or in the real world as a result of using digital technology, documenting the consequences for companies and any remedial action.

The first case study in the Digital Dangers series addressed Corporate Responses to Hate Speech in the 2013 Kenya Presidential Elections, focusing on the experiences of the Kenyan telecoms operator Safaricom[2]. Future studies in this series will explore the economic and social impacts of network disconnection in Pakistan, human rights challenges for game console developers, and the challenge of protecting the free flow of information for international trade and human rights.

Lucy Purdon, IHRB's ICT Project Manager, prepared this paper with input from Salil Tripathi, IHRB Senior Advisor on Global Issues, and Motoko Aizawa, IHRB Managing Director USA.

IHRB wishes to thank the Ministry of Foreign Affairs of the Netherlands and the Ministry of Foreign Affairs of Sweden for initial funding for the Digital Dangers project. See www.ihrb.org/digitaldangers for more information.

1 http://www.ihrb.org/publications/reports/ict-human-rights-sector-guide.html

2 Available here: http://www.ihrb.org/publications/reports/digital-dangers-case-study-safaricom.html

Institute for Human Rights and Business
34b York Way
London N1 9AB
UK
Phone: (+44) 203-411-4333
Email: info@ihrb.org

ISBN: 978-1-908405-19-7

Contents

About this Paper

The ICT ecosystem is complex with different corporate roles and responsibilities. The aim of this paper is to clarify the role of a company like Ericsson, which is a network infrastructure vendor/solutions provider (defined as companies that build and manage the telecommunication network) within the ICT ecosystem. The paper discusses some of the challenges network vendors face in respecting human rights when their technology is misused by third parties, and explores the due diligence processes that could be put in place to reduce the possible risk of misuse, in particular regarding the interception of communications. This case study aims to:

- Unpack the roles and responsibilities of companies in the ICT sector, focusing on telecommunications vendors, which deliver products that enable communications to be intercepted as required by law.
- Advance understanding of the human rights challenges and dilemmas facing network vendors concerning unintended use of products and services, with a particular focus on the possible misuse of lawful interception.
- Highlight differences between lawful interception and mass surveillance products in the marketplace.
- Promote awareness of these challenges and dilemmas among multiple stakeholders, including business, government, regulators, civil society groups and the general public.
- Encourage transparency around company practices as outlined in the United Nations (UN) Guiding Principles on Business and Human Rights[3] , including steps to "know and show" that the company respects human rights.

What are potential risks to human rights as a result of the misuse of lawful interception systems? Telecommunication systems in most countries must include, by law, the capability to intercept communications, to assist law enforcement authorities in investigating and prosecuting crime. Law enforcement authorities typically obtain a warrant or legal order to intercept communications, depending on the country. The same technology may also be misused by those authorised to carry out interception, such as when specific groups (opposition parties, human rights defenders, ethnic, religious or sexual minorities) are placed under arbitrary surveillance, particularly in countries where legal oversight of interception is weak and where governments have a poor human rights record.

Human rights groups and the media have often criticised ICT companies that sell "surveillance" technology that enables governments to monitor communications. This criticism, at times, does not distinguish between misuse of lawful surveillance and the sale and design of tools designed to facilitate human rights violations via mass surveillance.

Some governments have used information gathered through these technologies to suppress dissent or commit other human rights violations. But "surveillance" has become a catch-all term to describe all sorts of technology, from standard telecoms equipment with legally mandated interception capabilities to the intrusive and often unregulated technology that enables, often arbitrary, surveillance on innocent individuals or help facilitate mass surveillance. While this paper is not addressing the deliberate sale of the latter, this is an important distinction, particularly as debates around government surveillance practices and corporate involvement continue following the Snowden revelations.[4]

IHRB approached Ericsson, a network vendor and service provider, to participate as the subject of this case study. Ericsson is a Swedish multinational company founded in 1876 and a market leader in its field selling standard GSM

3 http://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_en.pdf

4 http://www.theguardian.com/world/series/the-snowden-files

equipment.[5] 40% of the world's mobile traffic is carried over Ericsson networks. It employs over 115,000 people and operates in 180 countries, with net sales of SEK 227.4 billion (around US$ 34.9 billion) in 2013.[6]

Ericsson's 2013 Sustainability and Corporate Responsibility (CR) report describes three segments of Ericsson's business:

- Networks (the infrastructure that is the basis for all mobile communications);
- Global Services (managed services, consulting, and systems integration, customer support, network design and optimisation and network rollout);
- Support Solutions (software for operations support systems and business support systems, TV and Media Management, and m-commerce, or mobile commerce). [7]

In 2012, Ericsson sold to Sony its stake in the joint venture SonyEricsson, which manufactured handsets. Ericsson is no longer associated with the sale of mobile phone handsets but a perception remains among the public that the company is still active in this area.

Ericsson's operations include sales to and presence in several countries where human rights protections are weak and where legal rules governing interception of communications may be underdeveloped and/or in conflict with international human rights standards. Ericsson has raised the issue of how lawful interception could potentially be misused in its report, "ICT and Human Rights: An Ecosystem Approach".[8] Ericsson has experience of tackling a range of challenges regarding possible misuse of its products. This paper draws on examples from Iran, Syria, Georgia and Belarus.

Ericsson says its global presence makes it well placed to develop connectivity in ways that respond to the needs of particular communities and helps bridge the 'digital divide'. Ericsson often partners with NGOs, UN organisations and local civil society organisations to deliver community outreach services related to ICTS, utilising technology for positive realisation of human rights. Its initiatives include, for example, Ericsson's work with Refugees United which delivers a family reconnection service; Connect to Learn, a program to enable access to secondary education of girls; and providing emergency telecom services to assist with responses to disaster and humanitarian crises through its Ericsson Response program.[9]

IHRB wishes to thank Ericsson for its co-operation in preparing this case study. Ericsson representatives facilitated IHRB access to Ericsson premises in Stockholm and arranged interviews with Ericsson staff across a number of departments. This report consists of information from this series of interviews supplemented by IHRB research. Ericsson staff

5 Global System for Mobile Communications. GSM explanation from GSMA website. http://www.gsma.com/aboutus/gsm-technology/gsm "GSM (Global System for Mobile communications) is an open, digital cellular technology used for transmitting mobile voice and data services."

6 Full year 2013 figures taken from http://www.ericsson.com/thecompany/company_facts/facts_figures

7 Ericsson Sustainability and Corporate Responsibility Report 2013, Technology For Good, http://www.ericsson.com/res/thecompany/docs/corporate-responsibility/2013-corporate-responsibility-and-sustainability-report.pdf p3

8 Ericsson, ICT and Human Rights: An Ecosystem Approach, http://www.ericsson.com/res/thecompany/docs/corporate-responsibility/2012/human_rights0521_final_web.pdf

9 Read more in the Ericsson Sustainability and Corporate Responsibility Report 2013, Technology For Good, http://www.ericsson.com/res/thecompany/docs/corporate-responsibility/2013-corporate-responsibility-and-sustainability-report.pdf p45

submitted comments on drafts to ensure accuracy. Ericsson provided no financial assistance to the preparation of this study. This study reflects the views of IHRB and not of any company quoted in the study.

The telecommunication network is a technical subject. This paper is not an investigation into the technology per se, but rather analyses the roles and responsibilities of network vendors and what policies and processes could be put in place to reduce the risk of misuse of these products by third parties. Ericsson was one of the first telecommunications companies to publicly commit to implementing the UN Guiding Principles on Business and Human Rights, which the UN Human Rights Council adopted in 2011. One of the core elements of the UN Guiding Principles is that companies must undertake human rights due diligence, an on-going process through which the company "knows and shows" it is respecting human rights in practice. Ericsson's due diligence process with regard to sales is detailed throughout this paper as an illustrative case study.

A list of further resources with more detailed technical explanation features is provided at the end of the report for readers wishing to explore these issues in more detail.

Methodology

IHRB researcher Lucy Purdon spent 7 days at Ericsson's headquarters in Stockholm, Sweden, to conduct research for this paper. Ericsson co-operated with IHRB's request to visit the company headquarters and made its staff available for interviews. IHRB spoke to several departments including Sustainability and Corporate Responsibility, Sales and Marketing, Communications, Technology, Product Security, Government and Industry Relations, Research, Business Management, Trade Compliance, and Regulatory Solutions, the latter of which includes the team responsible for Lawful Intercept solutions.

Each department interviewed identified potential human rights risks or challenges for the company linked to the use of its products and services. This was followed by a discussion about Ericsson's actions to minimise such risks. Discussions included the way the company took decisions, the governance and due diligence framework it applied to these decisions, and the impact of those decisions. IHRB shared its draft report with Ericsson before publication in order to identify any proprietary information or information of commercial significance that should remain confidential, as well as to ensure accuracy. IHRB would like to thank all representatives of Ericsson who were interviewed for their co-operation and willingness to participate in this study.

The study reflects the views of IHRB and not those of Ericsson.

Executive Summary

This study focuses on the network vendor, a company that builds and services the infrastructure of a network. The human rights challenges such a company faces are different from those that other companies in the ICT sector face. Network vendors do not directly work with consumers. Their business arrangements are usually with telecommunications operators (e.g. companies that operate mobile or terrestrial phone networks) and on occasion government departments.

Vendors face challenges often bound up in the functionalities of networks. For example, a basic functionality of mobile telephony is to ensure that a network can locate a device for the purpose of making and receiving calls and other related services. Without this inherent feature, there would be no connectivity. As large numbers of people now carry mobile phones that can pinpoint a location at any given time, law enforcement have a powerful tool that can assist in their work, for example to enable tracking of missing persons. However, there is also some evidence of this functionality being misused where States use location tracking to locate activists and political targets for purposes of harassment or arbitrary detention. Mobile phone technology has unfortunately become increasingly dangerous for activists in some countries.

As part of delivering telecommunications networks, operators are usually required under local law of many jurisdictions to provide the technical means for individual communications to be intercepted for the purposes of legal investigations of criminal activity. Legally mandated interceptions of communications may be for legitimate purposes, but may also be misused when government actors place specific groups (opposition parties, human rights defenders, ethnic, religious or sexual minorities) under arbitrary surveillance.

Reducing the risk of misuse of these systems is one of the challenges for the network vendor, one this paper focuses on. When an operator or government misuses lawful intercept solutions, the network vendor is often accused of being linked to an abuse of human rights through its operations, and thus negatively impacting rights. If the government responsible for the misuse is perceived to be a repressive regime, this increases scrutiny on the network vendor by human rights groups.

Companies such as Ericsson, which provide networks are expected to adhere to a strict set of rules regarding interception and are working to minimise any possible misuse. Ericsson has stated that it would categorically reject supplying mass surveillance technology and has in place a number of mechanisms to cope with the risks of misuse of its network technology.

Research referenced in the paper has shown that some companies are marketing and selling products that are much easier to misuse than regulated lawful intercept technology, to regimes with poor human rights records. This part of the ICT industry is highly secretive and can cause problems ranging from reputational to legal, for network vendors providing legally mandated and regulated interception technology. This is because network vendors can become embroiled in accusations of mass surveillance when a particular government is found to use such technology, and such technological capability may even be added by a third party onto a network sold by a vendor with or without the vendor's consent.

This study discusses Ericsson's pre-sale due diligence process and reflects on how human rights risk management is embedded into the company's operations in the form of a Sales Compliance Board. The analysis also looks at the processes put in place by Ericsson to limit misuse of lawful intercept systems, including a system designed to limit the number of people that can be intercepted simultaneously; an interception warrant database; seeking end user statements from customers, and training of operator personnel.

As States change their laws to expand interception capabilities, telecommunications companies will increasingly face demands to provide the technology to facilitate this. Such changes to legal systems can undermine protection of existing state human rights obligations and a challenge can be determining when lawful interception is over-reaching. Many states expect companies that are already providing network infrastructure to make such technological solutions available for broader surveillance with greater adverse human rights impacts. As a vendor and a company that builds network infrastructure, Ericsson could face demands for increased capability of this kind or to provide direct access to end users, sidestepping the operator and reducing the opportunities for vendors to mitigate the risk of misuse.

Although the UN Guiding Principles on Business and Human Rights help business to implement systematic and on-going human rights due diligence processes, they cannot provide a solution for every dilemma that a company faces. With this reality in mind, a company should be prepared to work through dilemmas and mitigate risks by using tools such as:

Transparency: The UN Guiding Principles call on all companies to communicate with individuals or groups, as well as other stakeholders that may be impacted by their activities. Companies should strive to be as transparent as possible about the challenges they face and actions to address them.

Collective Action: The dilemmas presented in this study cannot be solved by individual companies acting alone. Companies should develop sector wide efforts to address shared challenges and work together towards significant change.

Regulation: Governments will need to clarify rules for companies providing technologies that can be used in ways that undermine respect for human rights and bear in mind their own duty to protect against human rights abuses involving non-state actors such as companies. Companies should advocate for responsible government action in this area.

Key Findings and Recommendations[10]

Key Findings

- Technical strategies form only some of the mitigation steps that a company should undertake to prevent misuse of its technologies. Also critical is training for network operators in correct use of equipment and in ensuring that customers effectively implement technical and security strategies.

- Regulators need to clarify the capabilities and the uses of technology that comprise lawful interception and also the limits of lawful surveillance. In recent years, an entire industry has emerged around providing lawful intercept solutions that are often unregulated, used by law enforcement agencies and others, which expand targeted, warranted action (as it is meant to be) into something resembling mass surveillance.

- While recognising the importance of location tracking for connectivity and a range of legitimate law enforcement purposes, it is crucial to note that such capabilities often do not have the same safeguards that apply to interception of content. This makes location tracking of people easier to misuse, particularly where legal oversight is already weak or where networks are insecure. As location data is collected more regularly for a range of services, regulatory or governmental clarity on additional safeguards, both on the technical and policy level is needed.

- States that change laws in order to expand interception capabilities present a dilemma for telecommunications companies. Operators face the option of either complying with new government demands or losing a contract and possibly their license to operate in some countries or territories. Although legal compliance in such cases is a matter for the operator, it impacts the vendor as well. Operators are often legally constrained from reporting on such issues, but some operators are starting to push back by disclosing more information that helps stakeholders understand the constraints placed on them by governments with regard to transparency.

- A network vendor is not an operator, and as such would not receive requests for lawful interception directly from a government. A network vendor therefore would unlikely publish a transparency report on this subject. However, there is still much to be learnt from vendors about the way different countries regulate interception of communications, what companies are being compelled to do, the technology that is being requested and how this can impact on rights to privacy and freedom of expression.

Key Recommendations for Vendors

- Network vendors such as Ericsson should publicly distance themselves from companies that describe their products and services as lawful intercept "solutions" when in fact they provide capabilities that go beyond this. Some of these companies market themselves by asserting that their technology can be added to a network developed by Ericsson or other vendors. Ericsson and other network vendors can take action by ensuring that their company's logo and name are removed from any marketing literature by such enterprises.

- In addition to due diligence steps focused on the sale of technology products and their capabilities, network vendors should ensure that equal attention is given to training of operator personnel as part of the sale of

10 More recommendations can be found at the end of the paper.

technology products, including lawful interception systems.

- Companies should utilise membership of forums like the Global e-Sustainability Initiative (GeSI) (of which Ericsson is a member) and the multistakeholder Global Network Initiative (GNI), which also hosts the Telecommunications Industry Dialogue on Freedom of Expression and Privacy. A collective industry-led statement or initiative from groups like these, highlighting the dangers of mass surveillance that unregulated use of technologies pose could encourage regulators to act to ensure that the most intrusive and offensive technology is not sold to governments to be used to undermine respect for human rights.

Key Recommendations For Regulators

- Regulators should impose restrictions on exports, as appropriate, where there is clear indication that a specific technology is likely to be misused. At the same time, they should be aware of the impacts of such restrictions on telecommunications networks, as some of the impacts could be negative for effective operations. This entails looking at export controls not exclusively in terms of national security but also adding a human rights dimension. Change can be slow, but export controls can work. For example, protocols governing the spread of chemical weapons have prevented trade in certain chemicals to certain countries.[11] Likewise, the trade of nuclear technology is highly regulated through the non-proliferation treaty.[12] The Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES agreement)[13] imposes stiff penalties in trade of wildlife products. By the same logic, export controls can be developed to prevent the spread of surveillance technology from falling into the wrong hands, and lawful intercept technology from being misused.

- Regulators should clarify the technological capabilities and uses that are justifiably part of a regulated lawful intercept functionality, so that companies selling technology that go beyond these standards do not promote themselves as lawful intercept solutions providers. Where the human rights situation warrants it, such exports or sales should not be permitted.

11 See http://www.opcw.org/chemical-weapons-convention/

12 See http://www.un.org/disarmament/WMD/Nuclear/NPT.shtml

13 See http://www.cites.org/

1. Mapping the ICT "Ecosystem" : Roles, Responsibilities and the Challenges of Lawful Interception

The ICT sector is made up of many types of companies delivering products and services, which have been described as an "ecosystem". Understanding the role of each part of the sector, from telecommunications companies to web-based services, manufacturers of end user devices, components, and software, is crucial to identifying potential negative impacts the ICT sector can have on human rights.[14] It also enables companies to take appropriate steps to minimise these risks. For the purposes of this report and the issue of lawful interception, it is important in particular to clarify the roles and responsibilities of the government/regulator, and to distinguish the legal responsibilities of the network vendor from those of the *telecoms operator*.

Key Term: Lawful Interception

The European Telecommunications Standards Institute (ETSI) is an independent standardising body and has taken the lead in standardising lawful intercept technical requirements. Although defined as a regional standardisation body, ETSI standards do not just cover Europe, but are also widely applied worldwide. They define lawful interception as,

" A security process in which a service provider or network operator collects and provides law enforcement officials with intercepted communications of private individuals or organisations."

See: http://www.etsi.org/index.php/technologies-clusters/technologies/security/lawful-interception

The UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism described in a recent report the characteristics of lawful interception as:

- The targeted surveillance of suspected individuals and organisations
- The existence of prior suspicion and prior authorisation (whether judicial or executive)
- An objective assessment of the necessity and proportionality of the contemplated surveillance

See: UN General Assembly A/69/397 23rd September 2014
http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf

14 See European Commission ICT Sector Guide for a further description of the segments of the ICT sector: http://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf

Government / Regulator

- Governments grant law enforcement agencies the power to intercept communications
- Governments create policy, legal measures, organisational structures and government institutions to co-ordinate a country's ICT interests
- Regulators have different roles and authorities across different countries, but most often grant licenses to telecommunications operators and allocate frequency and spectrum

Telecoms Operators

- Operators are consumer-facing companies that provide mobile and Internet services for a fee
- Operators enter into an agreement with governments to provide telecommunication services
- Part of the agreement is to provide the capability for law enforcement to intercept communications (as long as there is such a law in the country)
- Any official requests for lawful interception would go to the operator, unless the authorities are directly connected to the network

Network Vendors

- A network vendor's main customers are telecoms operators
- Vendors are not consumer facing
- Vendors typically build, and in some cases manage, the telecommunication infrastructure that provide the basis for all fixed and mobile communications

Government/Regulator

Telecommunication systems in most countries must include, by law[15], the capability to intercept communications. In line with the ETSI and UN definitions referred to earlier, the concept can be broken down into:

- 'Lawful' – refers to rules and regulations governing who can access information, when and why.
- 'Interception' - refers to the technical act of interception.

However, what is "lawful" can differ from country to country, as outlined in the GNI report Opening the Lines comparing laws from the UK, Sweden and Russia, which demonstrates the variety and range of access and interception that is considered "lawful" in these countries.[16]

Intercepting communications is under particular scrutiny by civil society groups due to the impact of surveillance on privacy and many other human rights. The state has an obligation to protect rights of all citizens. In order to protect these rights, governments may have legitimate reasons to monitor the communications of certain individuals or organisations, for example, people who are legitimately suspected of planning to commit or having committed a crime, such as a terrorist act. But the same technology may also be misused by authorities, such as when specific groups (opposition parties, human rights defenders, ethnic, religious or sexual minorities) are placed under arbitrary surveillance, particularly in countries where legal oversight of interception is weak. There is evidence in some countries that technology is being used to track and detain political dissidents and as part of a wider pattern of intimidation, often with negative consequences or harm to the individuals.[17]

Telecoms Operators

The telecommunications industry is highly regulated. Telecommunications operators must have on-going relationships with governments, as they require licenses to operate and to obtain spectrum allocations. The contract to provide telecommunications services is between the government and the operator, therefore the legal obligation to provide interception capabilities (when such a law is in place) lies with the operator.

Interception and Legal Process

In Western Europe and the US, authorised law enforcement agencies seeking to intercept content of communications must first seek court or political authorisation and present a warrant to the operator. When a warrant is presented, the operator is obliged to provide interception and deliver or provide access to requested information.

In some countries, state intelligence agencies define interception procedures. In some cases, although warrants may be required for interception, they are not required to be presented to any party, and operators cannot ask to see

15 For example, providing the technical means for interception is a legal requirement for companies under a 1995 Council of the European Union Resolution on the lawful interception of communications, which allows lawful interception to assist law enforcement in investigating and preventing crime.

16 http://globalnetworkinitiative.org/sites/default/files/GNI_OpeningtheLines.pdf p10

17 Human Rights Watch (2014) They Know Everything We Do. Telecom and Internet Surveillance in Ethiopia http://www.hrw.org/reports/2014/03/25/they-know-everything-we-do See also the impact of surveillance on Bahrain activist and her family in UK High Court Judgment, case between Privacy International and HMRC. P18, Para 29 https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/privacy_international_v_hmrc_approved_judgment_12_05_14.pdf P18, Para 29 https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/privacy_international_v_hmrc_approved_judgment_12_05_14.pdf

them.[18] Intelligence agency control centres are often directly connected to the operator's network, enabling the intelligence agency to dip in and out of private communications at will.

In an effort to increase transparency around this practice, a growing number of telecommunications companies are releasing "transparency reports", which include information on the number and nature of requests for user data they receive from law enforcement. The kind of information given varies from company to company.[19]

The UK based telecommunications operator Vodafone recently released its first transparency report, called the Law Enforcement Disclosure Report[20], which focuses on the company's operations in 29 countries. This report confirms the dilemma that in some countries, the laws on interception have little or no legal oversight and allow law enforcement to bypass the operator and have direct access to the network. The report states,

"…In a small number of countries the law dictates that specific agencies and authorities must have direct access to an operator's network, bypassing any form of operational control over lawful interception on the part of the operator. In those countries, Vodafone will not receive any form of demand for lawful interception access as the relevant agencies and authorities already have permanent access to customer communications via their own direct link."[21]

Vodafone did not detail the countries in question due to concerns regarding possible retaliation against staff, but media reports state there are "about six" countries where the law obliges operators to install "direct access pipes" or allow governments to do so.[22]

Network Vendors

Network vendors such as Ericsson face human right challenges that are different from those of other companies in the ICT sector. The network vendor does not deal directly with issues involving third parties, such as requests to remove or block online content, or government requests for user information, or to suspend networks, as operators regularly have to face.

The role of the network vendor is typically to build, and in some cases manage, the telecommunication infrastructure that provides the basis for all fixed and mobile communications[23], including calls and data. A network vendor's main customers are telecoms operators. A network vendor ensures that connectivity can occur across services, operators, and borders, and is capable of handling the increasing demands for data and access, for example the

18 https://globalnetworkinitiative.org//sites/default/files/GNI_OpeningtheLines.pdf p12

19 See these examples of transparency reports, which each present information differently: TeliaSonera (Sweden): http://www.teliasonera.com/en/sustainability/transparency-report/ CREDO (USA): http://www.credomobile.com/transparency Telstra (Australia): http://exchange.telstra.com.au/wp-content/uploads/2014/03/Transparency-Report_2014.pdf

20 Vodafone Law Enforcement Disclosure Report, featured in Vodafone's 2014 Sustainability report http://www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf pp 61-81

21 Ibid p69

22 The Guardian, 6th June 2014 Vodafone reveals the existence of secret wires that allow state surveillance, http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance?CMP=EMCNEWEML6619I2

23 The most prominent standard for protocol description in the 2G era of cellular telecommunications is known as the Global System for Mobile Communications (GSM) See GSMA website for definition, http://www.gsma.com/aboutus/gsm-technology/gsm "GSM (Global System for Mobile communications) is an open, digital cellular technology used for transmitting mobile voice and data services." In addition there are systems for third generation (3G) and, more recently, fourth generation (4G) telecommunications networks and high-speed LTE (Long Term Evolution) standards for cellular networks, which allows faster connectivity.

growing demand for new media on devices connected to the Internet. A network vendor needs to be able to respond to events that affect the network performance. For example, if a country is to host a major sports event like the Olympic Games, this will put pressure on the existing infrastructure and the network operator will work on solutions for its customers to increase the capacity. Both a network operator and a network vendor continuously look for ways to optimise the network to ensure it can cope with increased demands for coverage and capacity.

Operators are bound by laws that require the provision of technical means to intercept communications for criminal investigations. As a result, network vendors run the risk of being exposed to the charge of being complicit in potential human rights abuses if the technical means for interception they have provided are misused. When building a network for an operator, Ericsson either hands over the management and running of the network to operator personnel, or manages the network on behalf of the operator. The latter is referred to as Network Managed Services [24]and can include handling requests for lawful interception that are passed to Ericsson from the operator.

A basic functionality of mobile telephony ensures a network can locate a device so that calls can be made and received and other services accessed from any location. Without this inherent feature, there would be no connectivity. Being able to locate a device also means being able to locate the person carrying the device, which is a powerful tool for law enforcement. This tool can be used for good, such as tracing criminal activity but it can also easily be misused. For example, technology can locate survivors of an earthquake based on the telephone signals they emit. But technology can also be used to locate individuals meeting peacefully in a gathering the government deems illegal. This misuse of an essential feature of mobile networks is one of the core challenges facing network vendors like Ericsson. As discussed later in the paper, there is no easy solution to prevent such misuse.

Separating Lawful Interception and Mass Surveillance in the Marketplace

Key Term: Mass Surveillance

In contrast to lawful interception, mass surveillance is understood to refer to the bulk access and/or collection of many users' communications without prior suspicion of individual targets. Therefore mass surveillance involves no individual target, no prior suspicion, is not time bound and due to the technology employed, potentially limitless. In contrast to technology provided for lawful interception, much of the technology for mass surveillance is unregulated.

The UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism wrote in a recent report on the use of mass surveillance for counter-terrorism purposes,

"Assuming therefore that there remains a legal right to respect privacy (and this cannot be disputed (see General Assembly resolution 68/197)), the adoption of mass surveillance technology undoubtedly impinges on the very essence of that right".

See: UN General Assembly A/69/397 23rd September 2014
http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf

24 http://www.ericsson.com/ourportfolio/products/network-managed-services

There is a difference between regulated telecommunications network infrastructure being misused, and products that are effectively "single use" that are used solely for illegal or improper purposes based on international standards[25]. The latter are largely unregulated, designed to be intrusive, and capable of intercepting a large number of people simultaneously. Vendors like Ericsson must adhere to the stringent ETSI standards when providing lawful interception systems that are designed to target individuals. Ericsson representatives interviewed for this study stressed that Ericsson seeks to minimise any possible misuse of its products, as discussed in more detail later in the paper. However, many other technology companies position themselves as lawful interception or intelligence specialists and many lawful interception solutions are available in the marketplace.

Although some companies say they are in the business of providing lawful intercept solutions, civil society groups have expressed concerns that a significant number of these companies may be selling technology that goes beyond regulated, targeted and controllable interception of individuals under prior suspicion and instead falls into mass surveillance of citizens or unregulated technology that is difficult to control. Examples include malware[26] that infects a target's computer and switches on webcams and microphones on devices, and zero-days[27], which exploits vulnerabilities in a computer application to enable hacking of communications, therefore reducing digital security for many others using the same application. The Canada-based NGO, Citizen Lab, which tracks where intrusive and so-called "single use" technology is deployed worldwide, wrote of the problem with connecting this type of technology to lawful interception:

"The term [lawful intercept] leverages the assertion that malware for surveillance and 0-days for hacking have the same status as statutorily mandated (and regulated) "lawful intercept" functionality in telecommunications equipment, when they are sold to government purchasers."[28]

Research[29] has shown that some companies are marketing and selling products to regimes with poor human rights records that are extremely intrusive and much easier to misuse than regulated lawful interception technology, such as malware.[30] Technology is even being used to target diaspora overseas that may be critical of the government concerned from afar. For example, Human Rights Watch reported that Ethiopians living in the UK, US, Norway and Switzerland have been targeted with malware, resulting in an illegal wire-tapping case in the US.[31] In one example in the same report, a Skype conversation recorded from an infected computer belonging to an opposition party member appeared on pro-government websites.[32] A criminal complaint has been submitted to the National Cyber Crime Unit in the UK over the sale of certain surveillance technology by a UK company to the government of Bahrain. The complaint alleges the technology was used by Bahraini authorities to gain remote access to the computers and mobile phones of 3 Bahraini pro-democracy activists living in the UK.[33]

25 "Dual use" is a legal term applied to products, services or technology that can be used for both military and civilian purposes. The term "single use" in the ICT sector is often used to describe technology that is considered to solely have the purpose of limiting the enjoyment of human rights. See Wagner, B (2012) Exporting Censorship and Surveillance Technology, p7. Available at: https://www.hivos.org/sites/default/files/exporting_censorship_and_surveillance_technology_by_ben_wagner.pdf

26 Software that is created and used to gain access to private computer systems, disrupt computer operations and/or gather sensitive information. Malware includes, for example, computer viruses, "Trojan horse" software and "worms".

27 An attack on a vulnerability in a computer application or operating system that developers have not yet addressed.

28 Citizen Lab, December 20th 2013, Shedding Light on the Surveillance Industry: The Importance of Evidence-based, Impartial Research

29 See Citizen Lab research https://citizenlab.org/publications/

30 http://surveillance.rsf.org/en/category/corporate-enemies/

31 See Kidane v Ethiopia https://www.eff.org/cases/kidane-v-ethiopia

32 http://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_0.pdf p80

33 See: https://www.privacyinternational.org/news/blog/bahraini-government-with-help-from-finfisher-tracks-activists-living-in-uk

The former UN Special Rapporteur on Freedom of Expression, Frank La Rue, stated in a recent report: "The corporate sector has generated a global industry focused on the exchange of surveillance technologies. Such technologies are often sold to countries in which there is a serious risk they will be used to violate human rights, particularly those of human rights defenders, journalists or other vulnerable groups. This industry is virtually unregulated as States have failed to keep pace with technological and political developments".[34]

In addition, a recent report of the UN Office of the High Commissioner for Human Rights on the Right to Privacy in the Digital Age states: "Mass surveillance technologies are now entering the global market, raising the risk that surveillance technology will escape government controls."[35]

A number of companies are either under investigation or involved in litigation in various jurisdictions over selling technology to regimes, which have used them to violate human rights.[36] For example, the technology assists authorities who wish to intimidate and silence those critical of government practice by imposing surveillance on the communications of people not suspected of committing a crime and who are exercising their right to freedom of expression and assembly. The use by governments of such technologies to assist intrusive surveillance of innocent people breaches their own obligation to respect and protect human rights.

There is a concerted movement involving civil society groups, governments, politicians, and academics in Europe to regulate certain ICT products and services, which can pose a risk to human rights. As technology moves rapidly, it can be a challenge for regulators to keep up with the speed at which products are developed and all the uses to which that can potentially be applied.[37]

As Ericsson is a leader in its field, many companies providing these products and services market themselves by pointing out how their technology is compliant with Ericsson's technology. For example, in the Surveillance Industry Index[38], a database of corporate material from companies currently suspected of supplying intrusive technology to governments with a poor human rights record, a number of featured brochures either mention Ericsson or use the company logo in marketing leaflets and manuals.[39] Companies like Ericsson run the risk of being associated with other companies that sell extremely intrusive surveillance technology which purports to offer lawful interception solutions but is actually capable of much more. Being associated in any way with unscrupulous companies will ultimately affect the vendor or operator. The vendor company providing lawful intercept capabilities risks finding itself associated with the company that facilitates mass surveillance, in particular if the vendor is a more recognisable entity or brand name, and will therefore more likely be linked with any resulting violation.

---

34 A/HRC/23/40 17th April 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf p20

35 A/HRC/27/37 http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf p3

36 http://business-humanrights.org/en/amesys-lawsuit-re-libya-0#c18496

37 The export control regime is complex and while this paper does not do a deep-dive into the complexity, it is an important part of the solution. For more information see Tim Maurer, Edin Omanovic and Ben Wagner (2014) Uncontrolled Global Surveillance: Updating Export Controls in the Digital Age http://newamerica.net/sites/newamerica.net/files/policydocs/Uncontrolled_Surveillance_March_2014.pdf

38 https://www.privacyinternational.org/news/blog/the-surveillance-industry-index-an-introduction

39 Gamma Group "Communications Monitoring Solutions", https://www.documentcloud.org/documents/810453-793-gamma-group-product-list-finfisher.html p6 | Gamma Group catalogue https://www.documentcloud.org/documents/810727-772-gamma-group-catalogue-3g-gsm-tactical.html p42 | Speech Technology Centre, Russia. Multi-channel call recording and monitoring centre https://www.documentcloud.org/documents/810419-1140-speech-technology-center-brochure-smart.html | Tracespan, Russia https://www.documentcloud.org/documents/810572-1214-tracespan-brochure-dsl-xpert-vdsl-xpert.html | Elaman https://www.documentcloud.org/documents/409325-188-201106-iss-elaman3.html

2. Delivering Lawful Interception Systems

In the days of fixed line technology, data collected would be limited to who called who from where, the duration of the call and the content of the call. Now, data can include voicemails, location information, and text messages recorded and read. In addition, online activity can be monitored, including emails sent or received, and websites visited. Today there is an array of data and interactions beyond phone calls that are managed via the network and can be collected and therefore demanded by law enforcement authorities.

In order to meet the requirements of law enforcement, a dedicated technological solution that can intercept communication lawfully is needed. The technical means of interception are highly regulated, and it is extremely sensitive work. Ericsson has therefore set up a separate department to manage lawful interception. Ericsson's technical requirements for lawful interception (LI) system architecture are defined by ETSI and consist of three parts:

1. LI functionality embedded in network elements that have access to and ability to collect, an intercept subject's data.

2. An LI administration and mediation system that manages the LI functionality in the network elements and hands intercepted information over from an operator's network to an authority's monitoring centre equipment.

3. The authority's monitoring centre equipment which receives, stores and processes the intercepted data.

As part of the research for this paper, Ericsson representatives stated that the company delivers the functionality as described in points 1 and 2 above of ETSI requirements. For Ericsson, providing the first functionality and the second system are considered standard delivery, where customers choose a specific "subset". That is, the lawful intercept functionality in selected network elements and the Interception Management system, which administers and supervises the LI functionality, is made available in an operator's network and delivers the intercepted data to an authority's monitoring centre equipment. Ericsson representatives interviewed for this paper stated that monitoring centres for authorities are not part of Ericsson's solutions. Ericsson only provides products for the operator, not the state authority or agency. Ericsson representatives also noted that the company never carries out interception on behalf of law enforcement or a government agency. Ericsson personnel would only carry out lawful interception under requests from the operator, as part of their Managed Services.

In contrast to mass surveillance, the purpose of ETSI standards is to ensure that intercepts are carried out in a controllable way. ETSI standards support the concept that interception is targeted and has a specific purpose. National laws may differ as to how the target is decided. Ericsson executives increasingly ask: "Under what conditions will we do business?" For example, if an operator requests a lawful intercept capability that is much stronger or sweeping than what Ericsson normally provides or considers necessary, or goes beyond permissible limits within European laws, Ericsson policy is to advise against such action. IHRB was not able to clarify what the company's possible responses may be in cases where its advice is not followed.

3. Designing Lawful Interception Systems to Reduce the Risk of Misuse

As noted, Ericsson builds systems for its customers, i.e. telecoms operators. Government requests for interception would be made to the mobile operator, which maintains the relationship with the government or law enforcement authority (depending on the law). If Ericsson has provided the system to the operator, then operator personnel will carry out the request. However, if the operator has contracted Ericsson to undertake Managed Services, then Ericsson may have to carry out official requests on the operator's behalf.

Ericsson representatives interviewed for this paper stated that lawful interception is not the best tool for governments wanting to conduct mass surveillance, as it is not developed for that purpose. An Ericsson official said the company does not provide technology with mass surveillance capabilities. When asked about the risk of misuse of lawful interception and what measures Ericsson has in place to reduce this risk, Ericsson representatives said that its lawful interception system has been deliberately designed to limit the number of people whose communications can be intercepted simultaneously. Ericsson said this is an industry standard and is not a unique practice to Ericsson.

Logging Warrants

Ericsson representatives also described a logging database for interception requests. Legal warrants or orders for interception are presented to an operator by whichever authority is authorised to do so in a particular country. Each warrant may be logged individually in a database via a graphical user interface or via an API (a programming interface). If the legal system in a country does not require a legal warrant or order, the same information about the target is inputted to the database, but without any control of the legality of the request. Any additions or changes to this warrant database are also logged. This enables the operator to prove what has been done and what has not been done in the operator domain. When there is an alleged misuse case such record-keeping allows investigators to find out what happened and how. Also in validating an interception, the log is needed to prove completeness of information, i.e. that an interception actually was active at a specific time. The information is stored in an encrypted and access-protected log, which is only to be opened in case of disputes over what has and what has not been done or when ordered to do so by courts. Ericsson provided an example of a dispute where a politician's communications were intercepted and the content made public. The operator in this case was blamed for allowing this to happen, but due to the logging system in place, the operator was able to prove the interception was not initiated by them.

Managed Services

Ericsson representatives also said that if a company only sells the product then it has less influence over how it is used. In cases of managed services tied to the implementation and use of the product, the company has greater leverage, and has greater opportunity or influence to ensure the product is not misused. The contract negotiations here are crucial. Once the contract is agreed, it is important the delivery personnel has the correct training to ensure the contract is fulfilled and there is a clear escalation process in case of any uncertainties. In addition, regulators can play an important role in reducing the risk of misuse. States should ensure that regulators keeps pace with technological developments, including by clarifying interception standards and exploring limits on the maximum capability for interception. For example, should there be limits on how many phone numbers can be intercepted in a system? If a government demands more capability, under what conditions can this happen and how should a government be expected to justify such actions? These and other questions go beyond a company's contract with the government, highlighting the need for a broader public policy debate concerning how government decisions in this area should be accountable to the people.

4. The Use of End-user Statements

When Ericsson does business with an operator from another country, its Group Trade Compliance department has the responsibility for ensuring that relevant trade laws and regulations are followed. Ericsson's trade compliance team has members in different regions who cover individual countries and advise clients as to customs regulations and export controls. Ericsson secures "end user statements" from customers regarding all products, specifying its products cannot be re-sold or re-exported without the permission of the Swedish government (or a Government of another country where the export occurred). It should be noted however that a customer would most likely go through Ericsson as opposed to approaching the government directly. Customers are required to sign the agreement affirming they will use the product for its intended purpose - specifically "civil and peaceful use". In view of best practice from other companies faced with possible misuse by end-users (see the boxed example below), there may be further scope to strengthen or tighten its language in such statements. End-user statements have been a requirement from Ericsson for some time[40], but only in the past five years has customer understanding increased concerning why these statements are necessary and fit into the overall picture of import/export controls.

Ultimately, if Ericsson discovers its product was misused, its representatives would remind the customer of its obligation in the signed statement and explain that if it is not adhered to it would jeopardise future sales as authorities will not likely grant further export licenses to the end user, or may even remove existing licenses. If the situation does not improve, Ericsson may involve the competent export control authority that issued the relevant export license. In many cases for Ericsson this would be Sweden.

The Use of End User Agreements to Reduce the Risk of Misuse

The concept of end-user agreements is not unique to the ICT sector. Any company that is committed to respecting human rights should make it clear what its products are to be used for, and when misuse – actual or potential – is identified, it should take steps to distance itself so as not expose itself to the risk of complicity.

Taking an example from another industry, General Electric (GE), which manufactures medical equipment used by radiologists that can help medical practitioners identify congenital health problems in human foetuses found its product was being used in India by some practitioners to identify the sex of the foetus. As Indian society shows cultural preference for boys over girls, many families abort the foetus if the unborn child was a girl. The Indian government passed a law prohibiting it, but the practice continued. GE required practitioners buying the equipment to sign a bond saying they were aware of the law and would not breach it. The equipment itself carried a sticker mentioning the law and the penalty of misuse of the equipment. GE also launched a public awareness campaign and engaged the government of India to promote responsible business practices.[41]

40 End user agreements are not sought for customers within the European Union. In addition, an EU General Export Authorisation (GEA) can be applied for to export to Canada, USA, Norway, Switzerland, Japan, Australia, and New Zealand, which is valid for export from all EU countries, http://trade.ec.europa.eu/doclib/docs/2014/february/tradoc_152181.pdf

41 See Business Leaders Initiative on Human Rights (2010) The Millennium Development Goals and Human Rights: Companies Taking a Rights Aware Approach to Development http://www.hks.harvard.edu/m-rcbg/CSRI/publications/report_44.pdf pp47-53 and http://files.gecompany.com/gecom/citizenship/pdfs/ge_ethical_ultrasound_use_india_casestudy.pdf

5. The Challenge of Preventing Misuse of Location Tracking

Location information is of growing significance because of the sheer number of people around the world carrying mobile phones, which identify their location at any given time. Privacy advocates have been concerned for some time over the collection of location information.[42] Ericsson also noted in its ICT Ecosystem report that location tracking is an example of when telecommunications systems can be misused,

"Tracking capabilities in the [telecommunications] system of users ID and location may be misused by authorities, unlawful organisations and companies."[43]

Inherent in all mobile networks is the ability to find a user placing or receiving a call or message in order to connect. Without this inherent feature, there would be no connectivity. To send and receive phone calls or messages, mobile phones emit signals to nearby cell towers or base stations, which are able to pick up signals within a certain range. If the caller/receiver is on the move, say on a train, when the user moves out of range of one tower, the connectivity is maintained because the next closest tower picks up the communication. Mobile operators routinely collect this information mainly to use for billing purposes and to determine if a call was made locally, or while roaming nationally or abroad.

The French telecommunications operator, Orange, explains how location tracking works: "Location tracking works by tracing the radio base station (phone mast) that's providing the service. If only one base station is in range, you can be traced to a circular area around the mast. If more than one base station is in range, your signal can be 'triangulated' for a much more accurate position."[44]

Users can control certain aspects of location tracking, by consenting to have their location services activated to improve services related to applications such as search and maps. However, even if a user switches off location services like a Global Positioning System (GPS) in relation to these applications, this does not remove the ability for police and emergency services to be able to trace locations as signals emitted from the phone still reveal its physical location.

Information regarding a person's location can form part of the information collected during a lawful intercept. It is important to have access to such information in emergency responses, such as a kidnapping or identifying survivors in a natural disaster area. The ETSI Technical Specifications for Requirements of Law Enforcement Agencies sets out the requirements regarding location information:

42 The Chaos Computer Club, Europe's largest association of hackers, has provided information on and campaigned for greater privacy and digital security for over 30 years and raised concerns about the use of location data as far back as 2001. See Statement of the Chaos Computer Club to the EU Forum on Cybercrime, November 27th 2001, Brussels, http://dasalte.ccc.de/lobbying/statements/2001/CCC20011127.html

43 ICT Ecosystem paper, p9

44 http://studio.orange.co.uk/safety/mobile/241.html

"An LEA [Law Enforcement Authority] may request location information relating to locations, in a number of forms:

a) The current geographic, physical or logical location of the target identity, when telecommunications activity (involving communication or a service) is taking place;

b) The current geographic, physical or logical location of the target identity, irrespective of whether telecommunications activity (involving communication or a service) is taking place or not;

c) The current geographic, physical or logical location of an identity temporarily associated with a target service because of successful telecommunication or an unsuccessful attempt to establish telecommunication;

d) The current geographic, physical or logical location of an identity permanently associated with a target service.

NOTE: This information is expected to be made available from normal network operation."[45]

It is worth noting here that the ETSI standards reinforce that this information relates to a particular target, and not indiscriminate surveillance. It also specifies that location information pertain to the current location of a target.

The European Data Retention Act states that data, including location identification, should be stored for no less than 6 months and no more than two years.[46] However, the European Court of Justice recently found the Data Retention Directive to be invalid. At the time of writing, it is not yet clear how different states will review, adapt or discard data retention as part of their national laws. A statement from the Court said,

"The Court takes the view that, by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data. Furthermore, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the persons concerned a feeling that their private lives are the subject of constant surveillance."[47]

In the wake of revelations of mass surveillance carried out by the US and UK governments, among others, there is growing awareness of surveillance worldwide. The UN Human Rights Council has passed a resolution raising concerns over such surveillance.[48] Growing global awareness of the implications of bulk collection and storage of

45 ETSI, Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies ETSI TS 101 331 V1.1.1 (2001-08) Technical Specifications http://www.etsi.org/deliver/etsi_ts/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf 4.5, p10

46 Article 6 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

47 http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

48 The Right to Privacy in the Digital Age, A/C.3/68/L.45/Rev.1, 20 November 2013 http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1

location data[49] is evident as well as its possible misuse because collection and storage seems to be indiscriminate, and not targeted to specific individuals, or limited to current locations. While laws permit monitoring of specific individuals under certain circumstances, mass surveillance of the kind revealed by programmes such as Prism[50] in the US appears to contravene international norms and has been criticised as such by the UN Human Rights Council as well as US civil society groups and lawmakers.

In 2011, German Green Party politician Malte Spitz set out to demonstrate the power of location information by gathering his own location data from social networks and sued his mobile provider Deutsche Telecom to access his information, building up an interactive map which showed everywhere he had been and when he communicated over a 6 month period.[51] There is some evidence of how this functionality is being misused where states have used location tracking to locate activists and political targets. This has made activists increasingly vulnerable.

The 2013 Freedom on the Net report from Freedom House details a particular example from Sudan:

"The activist Mohamed Ahmed switched off his phone for a few days in early July 2012 to avoid arrest while in hiding from the NISS [National Intelligence and Security Service]. When he turned his phone back on as he was walking home to see his family, NISS officials roaming his neighbourhood managed to track his location based on the nearest telecommunications tower and arrested him later that night."[52]

One blatant misuse of location tracking occurred during the recent protests in the Ukraine following the government's decision to slow the integration process with the European Union. Protestors in the vicinity of one march in the Ukrainian capital Kiev were sent unsigned text messages reading, "Dear subscriber, you are registered as a participant in a mass disturbance".[53] It failed to disperse the protests and is reminiscent of the 2011 Egyptian revolution, where mobile operators were instructed by the government to send pro-Mubarak SMSs.[54]

In the case of the Ukraine, local service providers denied sending the message, and one insisted that the service was hacked and the messages were sent from a "pirate base station"[55] (it is not known if they had logged any request in a database as mentioned above). Ericsson has indicated that it is difficult to see what mitigation steps it can take from a technical point of view in such instances, apart from making the network more secure so that it can't be hacked and messages sent.

---

49 http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html

50 Prism is the code name given by the NSA to the programme that allows the NSA to collect information from internet companies, including emails and stored data. It is alleged the NSA has direct access to these companies' servers. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

51 http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz

52 Freedom House, Freedom on the Net 2013: Sudan, p14 http://www.freedomhouse.org/sites/default/files/resources/FOTN%202013_Sudan.pdf

53 http://thelede.blogs.nytimes.com/2014/01/22/ominous-text-message-sent-to-protesters-in-kiev-sends-chills-around-the-internet/

54 http://www.business-humanrights.org/media/documents/vodafone-statement-re-egypt-22-feb-2011.pdf

55 http://thelede.blogs.nytimes.com/2014/01/22/ominous-text-message-sent-to-protesters-in-kiev-sends-chills-around-the-internet/

A priority for network vendors is ensuring that networks are as secure as possible to prevent malicious attacks. Most cyber security threats are directed at websites or attempts to access people's personal information, such as bank details. Examples such as the one from the Ukraine, where it is claimed the network was hacked for the purpose of obtaining location information and sending text messages to people in the vicinity of a protest, show the potentially sensitive nature of location information and the importance of a secure network to protect human rights.

Without the ability for a network to locate a phone, there would be no connectivity, but this ultimately means a mobile phone is a potential tracking device. Location tracking or data often does not have the same safeguards that apply to interception of content, making it easier to misuse, particularly where legal oversight is already weak or where networks are insecure. As location data is collected more regularly for a range of services, a discussion on additional safeguards, both on the technical and policy level is needed to ensure protocols that prevent misuse of such location data.

6. Recent Human Rights Challenges for Ericsson

As stated earlier, Ericsson was one of the first telecommunications companies to publicly commit to implementing the UN Guiding Principles on Business and Human Rights. The company has taken many steps to make technology accessible in remote parts of the world. Ericsson believes the benefits of technology far outweigh possible risks to human rights. But because technology is mostly value-neutral, and because states can use technology to protect rights as well as to undermine their protection, Ericsson has found itself facing human rights challenges in high-risk areas. This has led the company to examine its practices in more detail and undertake rigorous due diligence to minimise the likelihood of such exposure in future.

The UN Guiding Principles say the responsibility to respect human rights applies throughout a company's global operations, and exists independently of whether the State meets its own human rights obligations. This section examines a few specific cases to illustrate the kind of challenges Ericsson has faced with regard to lawful interception. As noted earlier, media and human rights groups have criticised the company for supplying telecommunications systems to countries with poor human rights records, such as Iran, Syria, Georgia and Belarus.[56] Some reports alleged that Ericsson has sold technology to states that have in turn used it to spy on their citizens, or have used it to locate and interrogate dissidents and members of political groups that oppose the government. Not all such reports have proven to be entirely accurate. At the same time, such allegations indicate the importance for Ericsson to have a rigorous due diligence process to minimise risks and be transparent about what products the company sells to whom.

Ericsson says the company sells "standard GSM equipment"[57], which is the global infrastructure that enables connectivity. The company sells the same telecommunications systems to operators in all 180 countries where it does business. In interviews for this report, Ericsson representatives stressed that the network equipment is standardised and that its systems have the same functionality and technology globally. The company confirms that no products are customised for different markets. Ericsson is aware of the potential for certain products or services to be misused in ways that may violate human rights and its human rights policy requires it to undertake due diligence to take steps to ensure such misuse does not happen. As Ericsson's Ecosystem report notes,

"An unintended use [of lawful interception] can occur when an entity, such as a government, uses the feature to monitor the communications of citizens without the legal permissions that are required for such actions in other countries."[58]

The following incidents illustrate three different contexts in which Ericsson has faced challenges in this area:

56 http://www.humanrightsfirst.org/2011/11/18/excuses-excuses-surveillance-technology-and-oppressive-regimes/

57 Global System for Mobile Communications. GSM explanation from GSMA website. http://www.gsma.com/aboutus/gsm-technology/gsm "GSM (Global System for Mobile communications) is an open, digital cellular technology used for transmitting mobile voice and data services."

58 Ecosystem report, p14.

Who Sold What To Whom: Iran

Reports in 2011 claimed that Ericsson had sold " location tracking and text message monitoring"[59] to Iran's law enforcement or state security agencies, which had then been used to track and arrest political dissidents. In at least one case it was reported that the arrested person was tortured.[60] Ericsson denied it sold technology to Iran's law enforcement or state security agencies. The client was an Iranian operator, Irancell, the Iranian cellular operator and not the government itself or its security agencies. Ericsson sold a Location Based Charging (LBC) to Irancell, which the company stated is not able to track a caller in real time.[61] An Ericsson representative interviewed for this paper stated that, "LBC is used by operators all over the world as a marketing tool in order to charge customers differently depending on where they are located. LBC allows the operator to offer different charging billing packages. Ericsson is unaware of authorities in any country using LBC as an active monitoring tool (not least as typically this is not open to real-time analysis)."

However, media reports concerning this case made Ericsson acutely aware of the risks of being associated with some governments and clients, which are majority state-owned. A company spokesperson said in 2011,

"When the political unrest…intensified in 2009, we got a more restrictive approach towards doing business with Iran. And finally, in December 2010, we decided to not make any new deals."[62]

According to Ericsson's 2013 Sustainability and Corporate Responsibility report, the sale of "infrastructure-related products" to operators in Iran was to be phased out during 2013. However, as EU sanctions on financial transactions were relaxed at the start of 2014, Ericsson has stated that it intends to continue to engage with existing customers and explore opportunities with new customers in Iran. In parallel, in order to ensure adherence to the UNGP and responsible business practices, Ericsson has initiated a Ericsson decided to continue engaging with existing customers in Iran[63] and conduct a Human Rights Impact Assessment on their business relationships and operations in Iran[64] and will monitor international developments as they relate to Iran and its government. IHRB hopes that Ericsson will be able to share some initial findings once the assessment is completed.

Working In Conflict Zones: Syria

Syria has been in a state of civil war since 2011 and there are reports its government has misused the telecommunication systems in order to crack down on activists and protest groups.[65] This led to the US imposing financial and travel sanctions in 2012 against "those who perpetrate or facilitate "Grave Human Rights Abuses

59 http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html

60 Ibid.

61 http://www.thelocal.se/20111101/37098

62 http://www.stockholmnews.com/more.aspx?NID=7982

63 http://www.ericsson.com/res/thecompany/docs/corporate-responsibility/2013-corporate-responsibility-and-sustainability-report.pdf p15

64 http://www.ericsson.com/news/1776511

65 See Freedom House (2013) Freedom on the Net: Syria https://freedomhouse.org/report/freedom-net/2013/syria#.VGCQG9btnXQ

Via Information Technology" in Syria and Iran".[66] Also in 2012, the European Union banned the export of Deep Packet Inspection (DPI)[67] technology to Syria as part of its sanctions on the country because of the monitoring and interception capabilities, which were being used against dissidents[68], according to credible reports.[69] Ericsson has had Syrian telecoms operators as clients. When reports emerged alleging that Ericsson sold surveillance technology to the Syrian Government, Ericsson responded that the company sold "standard GSM equipment to operators in Syria and Iran, the same standard equipment that we sell to operators in our other 178 markets."[70]

An Ericsson representative interviewed for this report stated that,

"As of September 2011, in Syria Ericsson only engages with MTN[71]/Areeba since Syriatel was sanctioned by the EU. We stopped all deliveries, services and disengaged completely with Syriatel at the time the company was put on the EU sanctions list. We also sold equipment to the fixed line operator, STE[72], for many years. Since the political unrest began in 2011 our business in Syria - basically all business activities - have come to a standstill and been severely affected. In some areas we provide reconstruction support to MTN. The office in Damascus is closed. Some 25 employees are working from surrounding countries and 15 work from home."

Responding to Allegations of Misuse: Georgia and Belarus

Media reports have alleged that Ericsson sold "surveillance" equipment to Georgia and Belarus. Civil society groups had long held concerns that arbitrary surveillance was rife in both countries.[73] Thomas Hammarberg, the EU's Special Advisor on Constitutional and Legal Reform and Human Rights in Georgia, pointed to the high risk of misuse of telecommunications systems amid weak legal oversight.[74] Belarus, criticised for regularly harassing and

66 http://www.whitehouse.gov/the-press-office/2012/04/23/fact-sheet-sanctions-against-those-complicit-grave-human-rights-abuses-i

67 DPI scans data packets passing through a network and blocks or routes them to the intended destination. DPI is used to manage network traffic to help the network run smoothly and block the spread of viruses, but it is also possible to view personal information, search for keywords and block access to websites. For more info see: Wired, April 2012 How Deep Packet Inspection Works, http://www.wired.co.uk/news/archive/2012-04/27/how-deep-packet-inspection-works

68 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:016:0001:0032:EN:PDF

69 http://www.fidh.org/en/europe/france/15116-france-opening-of-a-judicial-investigation-targeting-qosmos-for-complicity

70 http://www.business-humanrights.org/media/documents/ericsson-resonse-re-surveillance-technology-oppressive-regimes-6-dec-2011.pdf

71 Mobile Telephone Network (South African telecoms operator)

72 Syrian Telecommunications Establishment

73 http://transparency.ge/en/blog/ending-unchecked-illegal-wiretapping-practices and http://www.indexoncensorship.org/wp-content/uploads/2013/01/IDX_Belarus_ENG_WebRes.pdf

74 http://eeas.europa.eu/delegations/georgia/documents/virtual_library/cooperation_sectors/georgia_in_transition-hammarberg.pdf see p21

arresting activists and journalists[75], began implementing the Russian SORM[76] surveillance system in 2010 and allocated around $1 million, to spend on traffic analysis alone.[77]

Ericsson was linked to this case because it had sold standard GSM equipment, that included the capability for lawful interception, to Georgian telecom operator Geocell in 2005, and had two operator customers in Belarus owned by Turkcell and Austria Telekom. It is not clear from reports if or what other surveillance capabilities were added by third parties on top of the standard GSM equipment Ericsson sold to the operators. But it is clear from these examples that when supplying any kind of technology to a state with a poor human rights record, particularly one which is known for weak legal frameworks and persecution of vulnerable groups, companies must be vigilant. They should be prepared to face scrutiny and potential criticism and therefore be transparent about which products have been sold, their capabilities, and the human rights due diligence undertaken before completing the deal.

Responding to accusations in Belarus in 2010, a spokesperson for Ericsson said,

"The possibility for lawful interception of traffic is incorporated in all the equipment we sell, and it is in line with the guidelines established by the Swedish Foreign Ministry, UN and EU."[78]

Responding to accusations in Georgia in 2013, Ericsson said in a statement that,

"The technology is aimed at lawful monitoring to fight crime, but the [Georgian] authorities allegedly use it for purposes it's not intended for."[79]

When asked about these incidents, Ericsson representatives have noted that their response might be different now, having worked for two years to understand and implement the UN Guiding Principles. Ericsson now acknowledges that it is not enough to state only that the company is abiding by national law. Ericsson states that it now works more actively in the sales process to reduce or mitigate human rights risks, and also in some cases works to undertake human rights impact assessments with more focus on stakeholder impacts and mitigation activities.

75 http://www.freedomhouse.org/report/freedom-net/2013/belarus#.UvKTMqXfCCY

76 SORM (literal translation, System for Operative Investigative Activities) is a surveillance system that allows security services tap into and monitor all mobile phone communications in real time. The modernising of the SORM system can be charted from the Soviet-era system that prevailed in the 1980s, when SORM was established to intercept fixed line communications. In 1996, SORM 1 was established to intercept fixed line and mobile communications. Two years later, SORM 2 was established to allow additional monitoring of the Internet, including emails and VOIP. Some reports (see below) say that Internet Service Providers (ISPs) and operators were required to install a "black box" on the network, which would allow the secret service to intercept communications directly. Around 2012 SORM 3 was established to allow collection and long-term storage of all other user communication data, including actual recordings and location.

77 http://www.freedomhouse.org/report/freedom-net/2013/belarus#.UvKRyKXfCCYhttp://www.indexoncensorship.org/wp-content/uploads/2013/01/IDX_Belarus_ENG_WebRes.pdf p18

78 http://www.dn.se/nyheter/varlden/ericsson-technology-used-to-wiretap-in-belarus/

79 http://www.thelocal.se/20131030/swedish-firms-help-georgia-spy-on-its-citizens-ericsson-teliasonera

The examples briefly discussed in this section represented different challenges for Ericsson. In Iran, the company categorically denies that it sold technology directly to law enforcement and intelligence agencies, as has been alleged. In Syria, the company confirms that it sold technology it would have provided in any country, and at the time of the sale, there were no export restrictions imposed on Syria by other countries. In Georgia and Belarus, Ericsson was public about the fact it had provided lawful interception capabilities, but did little to explain at the time what this meant and therefore quell suspicion that the company was 'helping' these governments use telecommunications to impose surveillance. Ericsson has a number of policies and processes in place now, including a Sales Compliance Board that brings together executives from several relevant departments and developed processes to conduct due diligence (as detailed below) to ensure that its actions respect human rights and a commitment to conducting human rights risk assessments, informed by these experiences, which are discussed in the next chapter.

7. How Ericsson has embedded the UN Guiding Principles on Business and Human Rights across the company

For Ericsson, transactions with governments with poor human rights records pose two significant risks – reputational and legal. Following on from the country examples discussed in the previous section, Ericsson undertook several measures, including the creation of a Sales Compliance Board. While no due diligence process can ensure that the steps a company undertakes are sufficient or adequate to eliminate all potential risks, the examples discussed in the previous section highlight why companies like Ericsson should have rigorous internal processes in place and should familiarise themselves with international human rights standards more thoroughly, including by constantly engaging with human rights experts, to ensure that its legitimate business activities do not contribute to human rights abuses.

Since Ericsson committed to implementing the UN Guiding Principles on Business and Human Rights, a number of changes in practices have been implemented. Ericsson says it found the Guiding Principles helpful because it made clear that human rights responsibilities exist through a company's operations and it was not just a supplychain issue, and that the company's operations can have an impact on a range of rights.

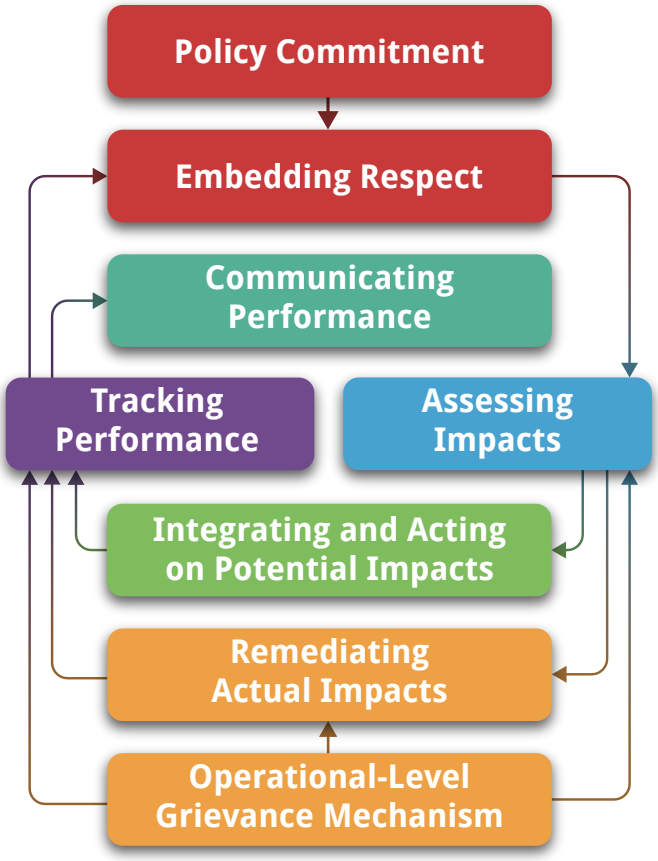

Illustration on previous page: An illustration of the relationship between the core elements of the corporate responsibility to respect human rights as set out in the UN Guiding Principles. Taken from the European Commission ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights.

Ericsson has taken the approach of reviewing and updating its Code of Business Ethics[80] as well as its Code of Conduct[81] to incorporate a reference and commit to implement the UN Guiding Principles throughout its business operations.

Ericsson has developed a pre-sale due diligence process, and human rights risk management is now embedded into Ericsson's operations in the form of a Sales Compliance Board[82] that brings together senior managers from many functional areas including Legal Affairs, Trade Compliance, Government and Industry Relations, Sales and Marketing, Communications, Business Units, and Sustainability and Corporate Responsibility. Decisions concerning certain sales, which may pose specific risks, are escalated to the Sales Compliance Board, which meets bi-monthly to determine specific policy guidelines and review cases, including based on potentially negative human rights impacts. Regional sales managers must request permission from the Sales Compliance Board for any deals involving three specific criteria: sensitive products, service and know-how, and sensitive customers or high-risk countries.

In the meantime, a core sales compliance team meets every two weeks to review and evaluate sales requests. The team draws on expertise from a number of functions and departments in order to discuss potential impacts and review policies. They look at the requests for sale of technology and services, which are approved, approved with conditions, or rejected. For example, a condition could be that Ericsson requires that implementing staff at the operator have the right training before a contract is concluded. Ericsson's view is that such an approach across a number of departments ensures that any decisions consider multiple angles and ultimately aim to reduce the risk that the company's technology directly or indirectly impacts negatively on human rights.

Risks to human rights are evaluated based on three criteria: 1) product, service or know-how; 2) market and; 3) customer.

Product, services or know-how: What is being sold?

Market: Where is the product/service going to be used?

Customer: Whom is the product/service being sold to?

80 Available here in 31 languages http://www.ericsson.com/thecompany/corporate_governance/code_of_business_ethics

81 http://www.ericsson.com/res/thecompany/docs/corporate-responsibility/coc/ericsson-code-of-conduct-en-rev-d.pdf

82 For more information see P15 of Ericsson's Corporate Responsibility and Sustainability Report 2013 http://www.ericsson.com/res/thecompany/docs/corporate-responsibility/2013-corporate-responsibility-and-sustainability-report.pdf

Ericsson uses a country risk list from an independent risk firm to identify high-risk markets and customers, from the perspective of human rights risks including freedom of expression, non-democratic policies, and corruption. The account manager in the country, who drives the sales, will know if the country where he or she operates is on the list. For certain countries, those working in the regions require permission from the Sales Compliance Board before making a sale. There are problems with any approach using country risk lists, and Ericsson is aware that the company needs to allow for the fact that the list is only updated once a year and political situations in any country can change quickly. The country lists are an input or a guide, but not a deciding factor on their own.

For example, social tension can rise and boil over rapidly in ways companies may not be able to predict as in the Ukraine in 2013. It is therefore important that in addition to the risk assessment, mitigation strategies are in place to prevent unintended uses of technology in the event of political change in a country.

8. How Should Vendors Respond When States Demand More Interception Capabilities From Operators?

So far, this report has analysed situations where governments or other buyers could potentially misuse lawful interception systems in ways that could have adverse impact on human rights. Ericsson has developed steps that it believes can help reduce risks, through strengthening the human rights due diligence process. Previous sections discussed cases where Ericsson is already taking technical steps, for example, by:

(i) Designing its lawful interception system such that it can only handle surveillance requests for a smaller number of people simultaneously, and
(ii) Requiring mandatory training for the operator to use the equipment in ways that comply with the law, and
(iii) Implementing technical and security strategies.

Despite these efforts, some States are developing laws that seek to expand interception capabilities and are increasingly asking telecommunications companies to provide the technology to do so. These changes reduce legal oversight and potentially go beyond the prevailing notion of what constitutes lawful interception, for example under ETSI standards, thus potentially undermining respect for existing state human rights obligations.

The report of the UN High Commissioner for Human Rights, The Right to Privacy in the Digital Age, reflects this concern and the risk for human rights,

"The enactment of statutory requirements for companies to make their networks 'wiretap ready' is a particular concern, not least because it creates an environment that facilitates sweeping surveillance measures."[83]

States expect companies that are already providing network infrastructure to make such technological solutions available. Operators must comply or risk losing a customer and possibly their legal license to operate. This also impacts vendors who build and service the networks for operators. In addition, weak laws and/or a lack of democratic control increase the risk of misuse of a powerful tool such as lawful interception technology.

In his report to the Human Rights Council in 2013[84], the former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, lists several common concerns regarding inadequate national frameworks including:

- A lack of judicial oversight;
- The expanding notion of national security, including the description of terrorism;
- Unregulated access by government agencies to communications data held by domestic service providers;
- Surveillance practices that fall outside the scope of legal frameworks, such as state-sponsored malware attacks;
- Extra-territorial application of surveillance laws to enable states to intercept communications in foreign jurisdictions;
- Mandatory data retention;
- Mandatory identity disclosure online laws, and;
- Restrictions on encryption and mandatory disclosure of encryption keys.

83 A/HRC/27/37 30th June 2014 http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf p14

84 A/HRC/23/40 17 April 2013 http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

These are key issues for companies building, developing and running telecommunications networks to evaluate, examine and consider. In countries where governance or human rights protection is weak, the risk of human rights abuses is heightened, and it becomes more challenging for ICT companies to meet their own responsibility to respect human rights.

A government can demand, via the operator customer, that Ericsson, as a vendor that builds network infrastructure, provide the state direct access. Some companies are willing to provide additional technology to the state that can increase surveillance capabilities on top of a network without questioning the government, regardless of consequences. For Ericsson, its executives say, this can pose a serious dilemma about the appropriate course of action it should take.

An example of such a dilemma can be seen in a case in which one of Ericsson's operator customers sought major changes to its telephone and Internet network. If Ericsson agreed to make such changes, it would have enabled the surveillance of a large number of people and allowed the government in question to collect and store much more data on citizens across all methods of digital communications than was otherwise possible. Ericsson states that it refused this contract.

According to interviews with Ericsson representatives, an internal legal review found that what the customers were asking for in this case was legal under recently expanded laws governing interception in that country. On the one hand, everything the customers were asking was legal under the laws of the country in question. On the other hand, the increased surveillance capabilities requested raised serious concerns for Ericsson about the potentially negative human rights impacts of such capabilities.

It is critical for Ericsson to have robust internal processes in place, and the company has indeed taken steps in this regard. Ericsson takes the UN Guiding Principles seriously. In the case of this transaction, Ericsson followed its set due diligence process. The transaction raised internal red flags due to the human rights risks it could pose. As a result Ericsson turned down the initial request. In making such decisions regarding sensitive transactions, in the future Ericsson needs to ensure its internal processes are robust so that it can evaluate the human rights risks such transactions pose, even when the transaction has significant commercial value.

The challenge for companies is ensuring that internal processes and decisions form part of a feedback loop that can help the company strengthen further processes and be prepared if and when similar requests come their way. If situations like the one described above become a trend, companies need to be prepared in how they will respond to such demands - how they will modify a request, accept and supervise, or turn it down.

In such a situation the onus is on the company to satisfy itself and its board whether it has analysed the situation sufficiently to ensure that the risks the transaction poses to human rights are not grave and that human rights may not be harmed. The company must keep in mind at all times that transactions in such cases run the risk of later being accused of complicity in human rights abuses that may follow.

Companies need to understand the context; they should examine the likelihood of human rights abuses occurring; and they should get access to all possible information on the basis of which it can make an informed decision. If the company's analysis reveals that human rights abuses are likely, that it is providing the technology that enables such abuses to occur, and that the company knows that the buyer is likely to use it in a way that leads to human rights abuses, then it needs to examine the transaction extremely seriously. As part of its due diligence, companies should seek assurances from the state or the buyer that the technology will not get misused, and that its use would be consistent with human rights standards. It is entirely possible that a government would be unwilling to provide such assurances. In such cases, a company like Ericsson has to think hard before deciding if the transaction is worth

undertaking, given all the potential risks.

These are not easy decisions. As Ericsson representatives noted during interviews for this report, although the UN Guiding Principles help business to implement systematic and on-going human rights considerations, they cannot provide a solution for every dilemma that a company faces. The Guiding Principles do however advocate transparency, and Ericsson should be commended for its willingness to be transparent about this difficult issue. This is an issue one company cannot solve alone. It will take a sector-wide effort to bring about significant change, and it will require governments to clarify the rules bearing in mind their own obligation to respect, protect, and fulfil human rights. A still small but growing number of operators are beginning to publish information explaining the often-complex laws they are bound to follow, and in some cases are speaking out against intrusive State surveillance.[85] Such steps are to be commended.

Disclosing such information is a sensitive matter for companies. As the Vodafone Law Enforcement Disclosure report revealed, legal restrictions in some countries prohibit disclosure of the technical aspects and capabilities of operating systems. Even disclosing information about how many requests companies receive is against the law in some countries. There is also the possibility that company employees may be placed at risk if information is disclosed.

It should of course be reiterated that the primary responsibility to protect human rights rests with the state. It is the state that changes laws, and it is the state that expands the definition of surveillance, its intensity, duration, and frequency. Companies providing technologies in this area need clarification when expanded surveillance laws at national level potentially undermine international human rights standards and a chance to raise concerns.

The concluding section offers a number of recommendations for network vendors and regulators.

85 See http://www.channel4.com/news/vodafone-shocked-spying-phone-gchq

Recommendations For Vendors

Based on the research conducted at Ericsson, the following points set out a number of recommendations for network vendors :

Embedding Commitment and Employee Awareness

- Establish a Human Rights Policy as the first step towards embedding human rights awareness in the company and build training for employees around it on risks to human rights.

- Train all staff on human rights policies, and ensure that mechanisms are in place through which staff may raise concerns about risks to human rights.

- Raise the issue of privacy with engineers at the first stages of product development and ensure they know they can flag any privacy related problems they discover when developing products or services.

- Ensure that product training for customer personnel follows agreed contractual terms and empower personnel to escalate to managers any instances of unauthorised data requests.

- Be part of collective action in this area by joining or utilising membership of fora like the Global e-Sustainability Initiative (GeSI) (of which Ericsson is a member) and the multistakeholder forum Global Network Initiative (GNI), which also houses the Industry Dialogue. An industry-led statement or campaign that speaks out against unregulated technologies used for mass surveillance could help efforts by regulators to ensure the most intrusive and offensive technology is not sold to governments with poor human rights records.

Escalation Process

- Involve company board of directors directly in any cases in which management is not able to make a firm decision about a specific transaction involving potential risks to human rights. Implementing a corporate human rights policy is ultimately a board-level responsibility and informed recommendations should be provided in line with the company's commitments.

- Companies should engage with their home government agencies, including Ministries of Foreign Affairs, and others, to seek guidance on difficult situations, and ask for bilateral interventions if necessary.

Process

- Companies need to know and show they respect human rights. This means companies should make human rights risk assessment part of the normal risk assessment procedures of the company, and conduct human rights risk assessments at regular intervals, throughout the life of business operations.

- Companies should be able to develop country-specific mitigation strategies to prevent misuse of technology in response to chaning political situations in a given country.

- Companies should be in regular dialogue with human rights experts and privacy experts externally, and form a cross functional human rights working group internally to ensure that human rights considerations are always

taken into account.

- Companies should ask host governments about their oversight policies and mobile operator customers about their processes for preventing misuse of lawful interception and assist in making them more robust.

- Companies should be transparent about the legal constraints they face in all countries in which they operate. By increasing levels of disclosure and explaining publicly what processes are in place to deal with state request, the company will be able to inform human rights groups and other stakeholders so that they in turn can seek legislative changes or mount legal changes to ensure there is sufficient oversight of interception.

Customers and Contracts

Companies involved in technology products should take into account the following considerations with respect to contracts:

- Take steps to prevent product misuse by using additional leverage provided in cases where the sales contract includes provision of managed services.

- Ensure that lawful interception training of personnel is provided alongside sale of products. This is an important part of due diligence, even the most secure product in the world won't be secure if it is installed incorrectly, making it capable of misuse.

- Require end user statements as part of all sales which detail approved uses of the product or service. This can help track products and performance. The language of the end-user statements should be clear. Include a statement that if the product is misused, any warranties/licence will be void, no on-going maintenance will be provided and the customer will be reported to the government where the company is headquartered, and the home government.

- Conduct due diligence on partners, including applying human rights criteria. In contracts with resellers and distributors, it will be important to include provisions for the reseller or distributor to conduct their own "know your customer" due diligence, and to provide for the voiding of any warranties if re-sale/distribution occurs without such due diligence having occurred. If circumstances allow, companies may need to consider selling directly if such risks cannot be effectively managed through contractual language and monitoring alone.

- Incorporate human rights safeguards into newly negotiated contracts and during contract renewal negotiations.

- Publicly distance themselves from the part of the sector that professes to be in the business of lawful intercept solutions but may also be selling technology that goes beyond targeted surveillance and falls into mass surveillance. Many companies that provide these products and services market themselves by pointing out how their technology is compliant with Ericsson's and other vendor networks. Vendors could take action, for example, by ensuring their company logos and company names are removed from any marketing literature. This is important not only for reputational purposes but also for legal reasons, to clarify, if questioned by authorities, the steps the company undertook to reduce the risk of being exposed to charges of complicity.

- Consider tools such as renewable licenses to create leverage and give the company an opportunity to review the situation and possibly take actions it otherwise could not if it delivered an open ended service.

Recommendations for Policy Makers

The issue of surveillance has gathered worldwide attention and should be of great concern to government and policy makers. The former UN Special Rapporteur Frank La Rue has expressed concern that the industry is driving the capabilities of mass surveillance. The capability to collect more and more data is increasing with developments in technology and regulation is not necessarily keeping pace. Therefore policy makers should take into account the following issues and questions:

- While there has been some movement in Europe on tightening export controls, regulators need to be clear what they want to achieve to avoid placing controls on products that could have a negative effect on running a network. This entails looking at export control for reasons beyond national security and adding a human rights dimension. Export controls can work –for example protocols governing chemical weapons have prevented trade in certain chemicals to certain countries. Likewise, the trade of nuclear technology is highly regulated through the non-proliferation treaty. The CITES agreement imposes stiff penalties in trade of wildlife products. By the same logic, export controls can be developed to prevent the spread of mass surveillance technology from falling into the wrong hands, and lawful intercept technology from being misused.

- Regulators should clarify capabilities with respect to regulated lawful intercept functionality, and prevent companies that are selling technology outside of these standards from offering such technologies for sale.

- Regulators should develop safeguards that reinforce the principle that surveillance is a highly intrusive act that must only occur under the most exceptional circumstances, as per the UN Resolution on the Right to Privacy in the Digital Age.[86]

A Note on Remedy

In a context where national law conflicts with or does not adequately incorporate international standards, the UN Guiding Principles on Business and Human Rights call on business enterprises to "seek to honour the principles of internationally recognised human rights when faced with conflicting requirements."[87] This is arguably one of the most challenging aspects of the Guiding Principles for companies to address.

A unique element of the ICT sector, which has not been fully explored in terms of the corporate responsibility to respect human rights, is the potential for remedies to be developed at a faster pace than other sectors. For example, an oil spill may take years to clean up and is extremely expensive. But with the ICT sector, some technology has limited shelf life. Some technology needs regular updating, sometimes weekly, from companies' central offices, or it needs license renewal. If those updates stop, the technology will not work efficiently or effectively, and that may prevent or reduce abuses. Companies and regulators can explore the possibility of reducing or switching off capabilities that can prevent a state with a poor human rights record from using technology in ways that were not intended.

86 UN General Assembly Resolution 68/197 The Right To Privacy in the Digital Age http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

87 UN Guiding Principles on Business and Human Rights, 23 (b) http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

Conclusion

Communications allow people, companies, and countries to get closer, leading to universal benefits to human rights and increased trade. But developments in communications technology are also making it easier for governments to violate the rights of their own citizens.

This paper focuses on particular challenges for one part of the ICT sector, but the wider challenge of strengthening privacy and the question of what reforms are needed in light of the Snowden revelations continues globally. State demands for surveillance capabilities are increasing.[88] Gaps exist where intrusive surveillance products are sold to governments with little or no legal oversight and blur the distinction of what is considered lawful interception and what is not.[89] New technologies and capabilities across the ICT sector will continue to present challenges in the future.

The technological and legal implications must be understood and addressed by the international community.

Parts of the telecommunications industry are highly regulated, nevertheless companies must undertake rigorous due diligence to ensure that their legitimate business activities do not harm human rights by their products and services being misused. Ericsson's due diligence process, as outlined in this paper, points to processes companies can embed into operations to give proper consideration to human rights risks. No doubt human rights due diligence for any company will evolve over time as a company learns from each deal made or refused and this information is used to strengthen and influence future business decisions.

Some states are seeking to expand the scope under which interception can be required[90] and this poses a particular difficulty for telecoms companies. It is difficult to establish "benchmarks" or "yardsticks" that can help a company determine if the due diligence it has undertaken is adequate or sufficient. A company should demonstrate that it has done all it can to minimise risk and has acted responsibly. This is important not only as a measure to preserve and protect a company's reputation, or to minimise the financial costs of having to pay compensation when things go wrong, but also to protect against legal risks.

Law enforcement, regulators and policy makers clearly have a difficult job but should not let claims of national security justify the excessive restriction of legitimate rights. When technology developed to keep us safe is then used against society, everyone loses.

88 For example, see http://globalvoicesonline.org/2014/08/15/russia-sorm-medvedev-social-networks-internet/

89 See Citizen Lab reports: https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/ | https://citizenlab.org/2013/10/igf-2013-exploring-communications-surveillance-indonesia/ | https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

90 Andrei Soldatov and Irina Borogan, March 2013 Lawful Interception: The Russian Approach https://www.privacyinternational.org/news/blog/lawful-interception-the-russian-approach

Further Resources

Human Rights in the ICT Sector

European Commission, ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights (2013)
http://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf

Ericsson, ICT and Human Rights: An Ecosystem Approach (2013)
http://www.ericsson.com/res/thecompany/docs/corporate-responsibility/2012/human_rights0521_final_web.pdf

Lawful Interception

GNI, Opening the Lines: A Call for Transparency from Governments and Telecommunications Companies (2013)
http://globalnetworkinitiative.org/sites/default/files/GNI_OpeningtheLines.pdf

Access Now, Commonwealth Of Surveillance States: On The Export And Resale Of Russian Surveillance Technology To Post-Soviet Central Asia (2013)
https://s3.amazonaws.com/access.3cdn.net/279b95d57718f05046_8sm6ivg69.pdf

Export Control

New America Foundation/Open Technology Institute/Privacy International/DigitaleGesellSchaft
Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age (2014)
https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/uncontrolled_surveillance_march_2014.pdf

Surveillance

Human Rights Watch: They Know Everything We Do. Telecom and Internet Surveillance in Ethiopia (2014)
http://www.hrw.org/reports/2014/03/25/they-know-everything-we-do

Citizen Lab, Mapping Hacking Team's "Untraceable" Spyware
https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

Citizen Lab, Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns
https://citizenlab.org/2013/12/syrian-malware-campaigns/

Citizen Lab, For their Eyes Only: The Commercialisation of Digital Spying
https://citizenlab.org/2013/04/for-their-eyes-only-2/

Citizen Lab, Planet Bluecoat: Mapping Global Censorship and Surveillance Tools
https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/

Institute for
Human Rights and Business

Shaping Policy ▪ Advancing Practice ▪ Strengthening Accountability

ISBN: 978-1-908405-19-7

Institute for Human Rights and Business
34b York Way
London N1 9AB
UK

Phone: (+44) 203-411-4333
Email: info@ihrb.org