Designing a Legal Regime for Lawful Interception and Government Access to User Data:

The Characteristics of a Rights-Respecting Model

Occasional Paper Series
Paper Number 5

JANUARY 2016

Institute for
Human Rights and Business

Published by IHRB.

Institute for Human Rights and Business
34b York Way
London, N1 9AB, UK
Phone: (+44) 203-411-433
Email: info@ihrb.org
Web: www.ihrb.org

Cite as: Institute for Human Rights and Business, "Lawful Interception and Government Access to User Data: Designing a Rights-Respecting Model" (Jan. 2016). Available at: http://www.ihrb.org/publications/reports/lawful-interception.html.

Acknowledgements: This Paper was written by Susan Morgan, with input from Lucy Purdon, IHRB ICT Project Manager, and Margaret Wachenfeld, IHRB Director of Research and Legal Affairs.

Susan Morgan has twenty years' experience working in both the public and private sectors. For the last fifteen years she has worked with or in the technology sector. Now a London based freelance consultant, she was the first Executive Director of the Global Network Initiative, a multi-stakeholder initiative focused on the responsibilities of technology companies to protect the free expression and privacy rights of their users when receiving government requests around the world. Susan worked previously with BT including six years focused on corporate responsibility, leading on strategy, policy and public reporting.

In the preparation of this paper a number of people were interviewed from different stakeholder groups including governments, companies and civil society. IHRB and Susan Morgan would like to thank them for their time, expertise and insights.

Lawful Interception and Government Access to User Data:
Designing a Rights-Respecting Model

January 2016

About this Occasional Paper

This is the fifth in a series of occasional papers by the Institute for Human Rights and Business (IHRB). Papers in this series provide independent analysis and policy recommendations concerning timely subjects on the business and human rights agenda from the perspective of IHRB staff members and research fellows. In this instance, the paper was written by Susan Morgan, with input from Lucy Purdon and Margaret Wachenfeld of IHRB.

The work to prepare the recommendations set out in this Occasional Paper began in response to ongoing developments in Myanmar, one of the fastest growing telecommunications markets in the world. In September 2015, the Myanmar Centre for Responsible Business (MCRB) and IHRB published a Sector Wide Impact Assessment (SWIA) on the emerging Information and Communication Technology (ICT) sector in Myanmar. The SWIA looks at the potential positive and negative human rights impacts of the sector for people in the country.[1]

At the time of writing the SWIA and this Occasional Paper, a key part of Myanmar's telecommunications framework governing lawful interception and government access to user data had yet to be finalised, leaving a significant gap in Myanmar's ICT regulatory framework. As it has opened up to foreign providers, the Government of Myanmar has made commitments to put in place a framework that respects human rights to govern how it will access communications content and data. The former military government established an intrusive surveillance regime for many years, both online and offline, in order to suppress criticism and dissent and restrict access to information for the Burmese people. The fear and threat of surveillance was part of Burmese life. Surveillance was widely conducted in the absence of a legal framework or oversight. There is now an opportunity for the new Government of Myanmar to develop a system that protects human rights, and to take a leadership position within the region.

The "Rights-Respecting Model for Lawful Interception and Government Access to User Data" presented here seeks to set out important principles for each step of developing and implementing a communications surveillance legal framework that protects and respects human rights. The adoption of the recommendations set out in the Model would help build trust in Myanmar's ICT services among users, service providers and other governments by being robust and aligned with international human rights standards.

[1] Myanmar Centre for Responsible Business (MCRB), Institute for Human Rights and Business (IHRB), and Danish Institute for Human Rights (DIHR), "Myanmar ICT Sector-Wide Impact Assessment" (2015).

While the Model focuses on work from Myanmar, it also reflects lessons learned from a broader set of countries that have faced similar challenges, drawing in particular from examples of the US and the UK. This Occasional Paper outlines the challenges and issues at stake and aims to provide further useful information for governments and other stakeholders involved in drafting legislation. The Rights-Respecting Model is relevant to any government seeking to put in place or modify its legal framework for lawful interception and government access to user data.

State surveillance practices have dominated debates in the ICT and human rights space since revelations in 2013 of the extent of these activities in some countries. At times, it is not an easy debate to follow; the legal frameworks surrounding surveillance are complicated, as are the concepts of lawful interception and communications data. This Paper therefore also aims to provide useful information and a description of the challenges for those with an interest in business and human rights and the technology industry but without specific expertise in these issues.

TABLE OF CONTENTS

Setting the Current Context: The Relevance of Human Rights to Lawful Interception and Government Access to Data 6

The Current Debate on Lawful Interception and Access to Data 6

Understanding Key Terms 7

Responses from Stakeholders to Increased Government Surveillance 8

Responses from Selected Governments 8
Responses from Companies 9
Responses from Civil Society 9

Lawful Interception and Government Access to User Data: Designing a Rights-Respecting Model 11

Purpose of the Model 11

Sources Used to Develop the Model 11

The Rights Respecting Model 13

1. Prerequisites to Communications Surveillance 13
2. Authorisation Processes 14
3. Oversight 15
4. Notification of Individuals 17
5. Remedy 18
6. Transparency 18
7. Provision for Framework Review 19

On-going Debates on Communications Surveillance 19

Mass Surveillance 20

Level of Protection of Communications Data 20

The Protection of Non-Nationals 21

Extraterritorial Reach of Surveillance 21

Conclusion 23

Setting the Current Context:
The Relevance of Human Rights to Lawful Interception and Government Access to Data

The Current Debate on Lawful Interception and Access to Data

The surveillance capabilities of countries are increasing. With the many different ways to communicate electronically, today there is a much greater array of data that can be collected and therefore demanded by law enforcement authorities. In the face of real or perceived national security threats, law enforcement and intelligence agencies have sought to harness the power of new communications technology and gather intelligence and evidence through digital surveillance to prevent attacks or prosecute suspected terrorists. At the same time, barriers to access communications services are decreasing, resulting in many more people carrying out more of their lives online. The dramatic decline in the costs of storing data online has further prompted moves to an online society. Some governments are taking advantage of these changes for purposes well beyond protecting national security or solving crime, purposes that are instead directed to controlling their citizens and maintaining power. As surveillance is often necessary on legitimate national security grounds, there is understandably secrecy around methods and even the laws that govern these actions. But that same secrecy can also mask serious violations of human rights.

The debate that followed the release of documents in June 2013 by Edward Snowden (a former contractor to the US National Security Agency (NSA))[2] centred on government use of surveillance powers in certain democratic countries, which had expanded largely without the knowledge of elected officials or the electorate. The revelations of extensive government surveillance prompted responses from numerous quarters to identify the most appropriate approach to balancing responses to serious security threats with obligations to protect human rights. It is often not an easy debate to follow as legal frameworks surrounding surveillance and the technical definitions therein are complicated.

In this age of widespread digital communications, the realisation of human rights, including the right to privacy, entails a complex balancing act between the obligations of governments, the responsibilities of companies that provide communications services[3] and the actions of users.[4] It can be argued that there is no respect for human rights in the absence of a secure society, and no security without respect for human rights. Governments have a duty to protect citizens from terrorism and other threats and therefore can have legitimate reasons to initiate surveillance of the communications of individuals suspected of a crime. But they must address the demands for security within the context of protecting other fundamental freedoms. Intercepting or monitoring communications is an intrusive process into someone's privacy and therefore a strict

[2] The Guardian, "The Snowden Files" (2013-2014)
[3] Such as telecommunications companies providing mobile services, Internet service providers (ISPs) and companies providing online services such as email, search, social networking and other messaging applications.
[4] See UN Resolution 68/167 The Right to Privacy in the Digital Age (21 January 2014), which affirms that the same rights that people have offline must also be protected online.

legal framework should govern such actions to prevent arbitrary violations of rights such as privacy and freedom of expression.

Understanding Key Terms

Lawful interception: Intercepting the content of communications in real time. "Content" refers to what was said during a phone call or what can be read in the content of an email or other type of digital message. Lawful interception is permitted in most countries under legal statute in order to assist with criminal investigations and the prosecution of serious crime, or to prevent national security emergencies. Usually, upon request from the authorities, a telecommunications operator collects intercepted communications of suspected private individuals or organisations and then provides law enforcement officials with access.[5]

Accessing communications data: Communications data (sometimes referred to as metadata but will be described as communications data in this paper) is generated as a person uses communications services. This is often known as the "who, where, when and how" of a communication. It is basically everything but the content and includes telephone numbers of caller and the recipient, the time and duration of a call, unique identifying numbers (each subscriber is allocated one, as is each mobile device), email addresses, web domains visited and location data. This communications data is important as it builds up a detailed picture of a person's life and movements, so intercepting the actual content of a call or email is not always necessary. [6] Communications data from modern digital communications can give more insight into a person's life than was historically the case when the only communications data available was telephone numbers and call duration information.

Mass surveillance: There is no international agreement defining what the term "mass surveillance" means. It is, however, understood by many experts 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 potentially limitless. UN experts have indicated serious concern about communications surveillance that is authorised on such a broad and indiscriminate basis. Actions of this scope are seen as running counter to the whole core concept of the protection of privacy that requires justification for intrusions on privacy to be made on a case-by-case basis.[7]

[5] See the European Telecommunications Standards Institute (ETSI) definition of lawful interception. The European Telecommunications Standards Institute (ETSI) is a 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.

[6] See further information on the definition and use of metadata/communications data from Privacy International.

[7] See the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40 (17 April 2013), para 54 and the Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37 Right to Privacy in the Digital Age (30 June 2014), para 27.

Responses from Stakeholders to Increased Government Surveillance

Responses from Selected Governments

At national levels, there are currently active debates on the future of surveillance. In the UK, for example, the draft Investigatory Powers Bill[8], intended to update and revise the UK's surveillance framework, was published in early November 2015. The bill is currently being scrutinised by a joint committee of the House of Commons and House of Lords and following Parliamentary scrutiny and debate it is expected it will be put to a Parliamentary vote in 2016.[9] The bill follows three reviews in 2015 of the UK's surveillance framework:[10]

- The Intelligence and Security Committee (ISC), the Parliamentary Committee that provides oversight on operational intelligence matters and the wider intelligence and security activities of Government,[11] published their report "Privacy and Security: A Modern and Transparent Framework" in March 2015.
- David Anderson QC, the UK's independent reviewer of terrorism legislation launched a major report, "A Question of Trust: Report of the Investigatory Powers Review" in June 2015 which made a number of recommendations on the future of communications surveillance in the UK.[12]
- The Royal United Services Institute (RUSI) concluded an Independent Surveillance Review, "A Democratic Licence to Operate",[13] in July 2015 concerning future requirements for the interception of communications.

These three reviews together produced almost 200 recommendations on surveillance reform, many of which are included in the draft bill.

In the USA, the US Freedom Act was enacted in June 2015 and restored several modified provisions from the Patriot Act that had expired. It is the first time since 1978 that a bill has passed Congress placing limits on the authority of the US Government to conduct surveillance. The Act requires greater oversight and transparency on surveillance practices including the declassification of Foreign Intelligence Surveillance Act (FISA) court opinions and effectively ends the bulk collection of phone records. But several other provisions exist in US legislation – Section 702 of the FISA Amendments

[8] UK Home Office, Draft Investigatory Powers Bill (November 2015).
[9] See IHRB's submissions to UK Parliamentary bodies conducting inquiries into the draft Bill: Parliamentary Science and Technology Committee (November 2015) The Joint Committee for Human Rights (December 2015) and the Draft Investigatory Powers Bill Select Committee (December 2015). See also Susan Morgan's submission to the Draft Investigatory Powers Bill Select Committee (December 2015)
[10] In addition to these reviews, In September 2014 Sir Nigel Sheinwald was appointed as the Special Envoy on Intelligence and Law Enforcement Data Sharing with a summary of his recommendations published in June 2015. See also the regular bi-annual report from the Interception of Communications Commissioner from July 2015.
[11] The Intelligence and Security Committee of Parliament (ISC) Privacy and Security, "A Modern and Transparent Legal Framework" (12 March 2015) p52, para 142 and 143 .
[12] David Anderson QC is the independent reviewer of terrorism legislation. In 2014 he was appointed to review investigatory powers in the UK with regard to the threats the UK faces, the capabilities required to combat the threats, the safeguards to privacy, the challenge of changing technology and issues relating to transparency and oversight. See, David Anderson, "A Question of Trust: Report of the Investigatory Powers Review" (June 2015).
[13] Royal United Services Institute (RUSI) "A Democratic License To Operate: Report of the Independent Surveillance Review" (July 2015).

Act[14] and Executive Order 12333[15] that authorise the bulk collection of data from people both inside and outside the US.

Responses from Companies

Companies providing mobile and Internet services are often caught in the middle: the mass surveillance revelations about government actions damaged the trust between ICT companies and their users, and between ICT companies and governments, creating tension between ICT companies and intelligence/law enforcement agencies. One response from companies has been to make changes to their systems to boost security and encryption, which is the technique by which data (when in transit or when at rest on devices) is scrambled to make it unreadable without using specific passwords or keys. This is creating further tension between technology companies and governments and looks set to continue. Many have suggested that the "crypto wars" fought in the US in the 1990's may well re-emerge.[16] Multi-stakeholder initiatives such as the Global Network Initiative[17], provide a forum for addressing some of these challenges and has developed a voluntary standard for companies setting out how they can respond to requests they receive from governments in a way that protects the rights of their users.

Responses from Civil Society

There have been robust responses from civil society groups, including public campaigns[18], forming coalitions and bringing legal action. For example, the Don't Spy on Us coalition was founded following the revelations by Edward Snowden, consisting of organisations working on freedom of expression, privacy and freedom of expression in the UK and Europe. They call for support of six key principles to end mass surveillance.[19] The International Principles on the Application of Human Rights to Communications Surveillance[20] were launched in 2014 after being developed by a wide range of civil society groups and technology experts globally.

Civil society groups have also launched several legal challenges to surveillance by intelligence agencies. At the time of writing, two cases brought by civil society groups are pending in the UK regarding network exploitation and hacking of devices by security services.[21] Ten human rights organisations worldwide have jointly taken a complaint to

[14] The US Foreign Intelligence Surveillance Act (FISA), Section 702
[15] Executive Order 12333
[16] This debate over encryption recalls the so-called "crypto wars" fought in the US in the 1990's, which many have suggested may well re-emerge. The Clinton administration proposed to compel all service providers give the government backdoor access to encryption keys by way of a "clipper chip". This was defeated by a coalition of civil society, academics and industry associations, but there are strong similarities between the 1990s debate and the current debate. For further reading see, Electronic Frontier Foundation (EFF), "The Crypto Wars: Governments Working to Undermine Encryption".
[17] www.globalnetworkinitiative.org
[18] See the US campaign, "The Day We Fight Back", February 11th 2014
[19] https://www.dontspyonus.org.uk/
[20] See also, the 2014 International Principles on the Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate Principles") developed by civil society groups and technology experts, which offer a comprehensive outline of the issues to be considered with regard to privacy and surveillance that support those outlined in this paper.
[21] See, GreenNet et al. v. Secretary of State for Foreign and Commonwealth Affairs and Government Communication Headquarters and
Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Government Communication Headquarters

the European Court of Human Rights regarding the surveillance practices of UK government agencies and the sharing of data with the NSA in the US.[22]

In the US, both the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) have filed lawsuits. At the time of writing, two are still pending[23], one is subject to appeal.[24] One case was dismissed.[25] A decision in the Court of Appeals for the Second Circuit in ACLU v. Clapper[26], regarding the mass collection of US citizen's phone records by the NSA, ruled the program violated Section 215 of the Patriot Act, which led to the amendment of Section 215 to prohibit the bulk collection of Americans' call records.

[22] See, Ten Human Rights Organisations V United Kingdom and Big Brother Watch, Open Rights Group, English PEN, Dr. Constanze Kurz vs. United Kingdom and Privacy International vs. United Kingdom
[23] See EFF case, Jewel v. NSA and First Unitarian Church v. NSA filed by EFF on behalf of a coalition of organisations.
[24] EFF and ACLU joined the council of appeal in Smith v. Obama.
[25] See ACLU case, Wikimedia v. NSA
[26] See ACLU v. Clapper.

Lawful Interception and Government Access to User Data:
Designing a Rights-Respecting Model

Purpose of the Model

One of the criticisms from the UN of most government surveillance frameworks concerns the *"lack of adequate national legislation and/or enforcement, weak procedural safeguards and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy".*[27] In addition, as communications surveillance is ostensibly carried out for the purpose of crime prevention or national security, it is often implemented in secret. This increases the importance of upfront consideration of potential adverse impacts on human rights associated with government requests and the need for appropriate legal protections.

This section proposes a Model for communications surveillance with recommendations for a legal framework that respects human rights and responds to weaknesses identified in current legal regimes. There is no "typical" process of accessing communications of individuals as processes differ from country to country. The Model therefore sets out important principles to guide the development or reform of legal regimes on communications surveillance.

Sources Used to Develop the Model

The Model is based on instruments and standards that require governments to protect human rights in accordance with international law and the international and regional human rights conventions they have signed and/or ratified. While numerous rights can and have been implicated in discussions around lawful interception and government access to user data under surveillance frameworks, there are three that are particularly relevant and the focus of this Occasional Paper and the Model presented. These are the right to security of person, the right to privacy and the right to freedom of expression (Articles 3, 12 and 19 respectively of the Universal Declaration of Human Rights).

The discussion in this section focuses on the right to privacy because it is particularly important in the context of lawful interception and government access to user data. The right protects private communications and sets out limits on the power of the State in relation to accessing those communications. However, under human rights law, the right to privacy is a qualified human right. This means that in specific and defined circumstances, such as those related to national security threats or other narrowly defined situations of public safety or crime prevention, governments may legitimately restrict the right and intrude on individual privacy provided a number of specific conditions are met.[28] In the report "The Right to Privacy in the Digital Age" presented to

[27] See Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37 Right to Privacy in the Digital Age (30th June 2014), para 47.

[28] The following rules apply to any restrictions on the right to privacy that governments seek to impose, including through communications surveillance. Any restrictions must not be either: (i) "**unlawful**": A restriction is "unlawful" when it is not authorised by States on the basis of national law specifically

the UN Human Rights Council (HRC) in June 2014, the UN High Commissioner for Human Rights highlights that authorities seeking to limit the right must show that proposed actions are connected with a legitimate aim.[29] The UN HRC appointed for the first time a Special Rapporteur on the Right to Privacy in July 2015 who can be expected to further define approaches to protecting the right to privacy in the digital age.[30]

The Model is also based on the UN Guiding Principles on Business and Human Rights – an authoritative global reference point setting out expectations for business and for government regulation of business in the area of human rights.[31] Companies are required to comply with the laws of the countries where they operate, but they also have responsibilities to respect human rights, whether or not these are set out in national law. There may be significant gaps in domestic legal frameworks or contradictory laws that contravene international human rights standards. In these circumstances, the expectation that companies will respect the human rights of their customers gives rise to challenges described in this Occasional Paper.

The Model also draws on recent reports to the UN General Assembly and Human Rights Council,[32] and other reports,[33] examples from national legislation, case law and discussions with experts. Country examples are included to illustrate relevant points. These examples are not necessarily presented as best practices, but instead as illustrations of different approaches to legal frameworks, reform and efforts to increase transparency.

---

authorising interference. The national law must be sufficiently accessible, clear and precise and also must not conflict with other provisions of the ICCPR, such as the prohibition on discrimination or the country's own constitution or (ii) "**arbitrary**". The protection against "arbitrary interference" means that the interference should be **reasonable** in the particular circumstances. It must be in **proportion to the aim** and the least intrusive option available to accomplish the aim and be **necessary** in the circumstances for reaching a legitimate aim.

[29] The limitation must also be shown to have some chance of achieving that goal while at the same time not being so overly restrictive that the restriction makes the exercise of the right meaningless. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary. See Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37 Right to Privacy in the Digital Age (30th June 2014), para 23.

[30] The United Nations Human Rights Council appointed Prof. Joe Cannataci as the first Special Rapporteur on the Right to Privacy in July 2015.

[31] See European Commission, ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights (2013).

[32] These recommendations draw on recent reports to the UN General Assembly and Human Rights Council, including the Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/HRC/23/40 (June 2013); The Right To Privacy in the Digital Age, UN Resolution 68/167 adopted 21st January 2014 ; Report of the Office of the United Nations High Commissioner for Human Rights, presented to the Human Rights Council A/HRC/27/37 (September 2014) and the Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism to the UN General Assembly A/69/397 (September 2014)

[33] David Anderson, "A Question of Trust: Report of the Investigatory Powers Review" (June 2015); Royal United Services Institute (RUSI) "A Democratic License To Operate: Report of the Independent Surveillance Review" (July 2015); The Interception of Communications Commissioner Office Annual Reports; IHRB Wilton Park conference report: "Tackling Dilemmas and Dangers in the Digital Realm" (November 2014); Freedom Online Coalition Working Group 3 Report, "Privacy and Transparency Online Draft Executive Summary" (May 2015)

The Rights Respecting Model

The Model follows the progression of a government request for communications surveillance – precursors before a request is made, the request itself, access to remedy and the opportunity for periodic review of legislation after requests are made:

1. Prerequisites to Communications Surveillance
2. Authorisation Processes
3. Oversight
4. Notification of Individuals
5. Remedy
6. Transparency
7. Provision for Framework Review

The Model is based on a number of important considerations:

- Legal frameworks should ensure that individuals know what information is being collected about them and what it is used for.
- Where surveillance is authorised, there should be clarity regarding the rules that govern the process.
- Effective oversight is essential, as is as much transparency as possible from both governments and companies.
- In cases where these steps are misused, either intentionally or otherwise, there should be redress and remedy.
- The expectations and responsibilities of companies in the ICT sector, in relation to both users and governments, should be examined as a matter of priority.

1. Prerequisites to Communications Surveillance

- Surveillance should be undertaken only when other potential measures that could have been used to deal with criminal or national security threats have been exhausted, for example other police measures that are less intrusive and have less impact on privacy.
- Any type of surveillance should be carried out only on targeted suspected individuals and organisations where there is prior suspicion that the targeted subject is suspected of a crime.
- Misuse of intrusive capabilities should be a criminal offence and surveillance used outside legal frameworks should be prohibited.
- The legal framework(s) for lawful interception and access to user data should be established through primary legislation and debated in the legislative branch, rather than being adopted as subsidiary regulations enacted by the executive. Public consultation and involvement of stakeholders is a vital part of the policy-making process because many of the related processes will be carried out behind closed doors, without the opportunity for public scrutiny.
- Embedding human rights principles into the regulation and laws that provide the framework for interception and surveillance is insufficient on its own. Accompanying the legal framework there should be more detailed regulations or codes of practice that set out more detail on how the law is intended to work in practice. Training should be provided for all agency representatives with powers to make requests to ensure the human rights implications of these activities are

clear and their obligations appropriately considered. Training the judiciary is also required.

- Where there is more than one law or regulation in place that authorises surveillance (e.g. telecoms, national security, tax, drug enforcement, cybersecurity laws, etc.) there must be consistency in the human rights safeguards in place across all laws. Clarity on which law has primacy in which circumstances is also of critical importance.

Country Example: Translating legislation into practice

One item worthy of note in the UK system is the existence of several Codes of Practice to aid in the implementation of the legal framework by those using the powers set out by statute. These codes currently include the Equipment Interference Code of Practice[34] and the Interceptions of Communications Code of Practice.[35] Experts giving evidence in response to the UK's draft Investigatory Powers Bill have stated that Codes of Practice are important and need to be presented to Parliament and regularly updated, so that stakeholders know how the legislation is being implemented in practice.

2. Authorisation Processes

- Specific instances of communications surveillance should be authorised by an independent and competent judicial authority prior to surveillance taking place (the Authorising Authority). Independence in this circumstance means separate and not connected to the authorities that will be carrying out the surveillance and competence means that those with responsibility for giving authorisation must have sufficient knowledge of the issues, both technologically and from a human rights perspective. This independence and competence is absolutely critical to the integrity of any legal framework.
- Some states have a process of Executive sign-off rather than judicial authorisation of requests. But the prevailing view among experts is that judicial authorisation is preferable for its independence[36] (see Country Example below).
- The legal framework should set out which agencies among government bodies can request lawful interception (the Requesting Agencies).
- Communications surveillance must be limited to that necessary to achieve a legitimate aim and use the means least likely to infringe rights – it must be both necessary and proportionate, as outlined earlier in the paper. An objective assessment of the necessity and proportionality of the contemplated surveillance should be a core part of the authorisation process. The Requesting Agencies must be required to consider the human rights implications of each particular surveillance request they make. This should include as a first step, consideration of whether any less intrusive methods are possible, to ensure that the issue of proportionality is addressed.
- The legal framework should also set out the criteria and conditions on which the Authorising Authority will decide on whether to authorise the request.

[34] UK Home Office, "Equipment Interference Code of Practice" (February 2015)
[35] UK Home Office, "Interception of Communications Code of Practice. Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000"
[36] European Court of Human Rights, Roman Zakharov v Russia, para 233; Court of Justice of the European Union, Digital Rights Ireland case, C-293/12, Grand Chamber, Judgement of 8 April 2014, para 62.

- Any authorisation should be time-bound, with a requirement that the Requesting Agency return to the Authorising Authority to request a renewal as that period of time expires; automatic renewals of surveillance requests should not be permitted.
- The legal framework should set out clear limits on the amount of time data collected can be stored and should require that collected and stored data is destroyed once that period expires. In addition, it should require that any data illegally collected is immediately destroyed and not used.

Country Example: Granting Authority to the Judicial Branch

In the UK, the Executive is responsible for authorisation of warrants. However in June 2015 the Anderson Review made a series of recommendations including the transferral of the power to grant warrants from the Executive branch to the judiciary for targeted interception and bulk warrants.[37] The UK's draft Investigatory Powers Bill proposes a new "double lock" on warrants in order to strengthen safeguards, so that warrants are signed by the Secretary of State and also subject to judicial approval. Some experts have questioned the role of the judiciary in this process who believe it is limited and provides insufficient protection or safeguards.[38]

3. Oversight

- Global debate continues concerning the best form of oversight of lawful interception and access to user data, but increasingly there is interest in mixed models of oversight that incorporate administrative, judicial and parliamentary actors.[39]
- Oversight must be vested in another body (or bodies) independent of the Authorising Authority that originally authorised the surveillance (the Oversight Body).
- Oversight must be rigorous and not a rubber-stamping exercise.
- Consideration should be given to permitting a confidential public interest advocate, for example an independent human rights expert, within the surveillance authorisation process to ensure that appropriate consideration is given to the human rights implications of requests. This is particularly important given the high degree of secrecy of authorisation processes that relate to national security.
- The Oversight Body must have access to all potentially relevant information to enable it to evaluate whether the state is carrying out its activities in a lawful way. This must include secret and classified information. Third parties, including companies, should have the ability to bring information to the Oversight Body where relevant.
- The Oversight Body must have the resources and expertise to be able to carry out effective oversight.

[37] D Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015) para 14 and 16
[38] See submissions to the Draft Investigatory Power's Bill Joint Committee from Liberty (para 6-9), Amnesty International UK (para 19-27), ARTICLE 19 (para 26-33).
[39] Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37 Right to Privacy in the Digital Age page 13.

- Within the oversight regime there must be regular reporting to the public on the appropriateness of the way in which the State is carrying out its surveillance activities that helps the public understand whether the State has followed the procedures set out in law.
- Oversight will usually happen at a defined time after surveillance has taken place (often with a regular report to the Parliament or public) and is designed to test whether surveillance that has already happened took place in accordance with the framework the country has in place.

Country Example: Illustrating Aspects of Oversight Models – United Kingdom

The Interception of Communications Commissioner[40] (IoCC) is appointed by the Prime Minister and is responsible for keeping under review the interception of communications and the acquisition and disclosure of communications data by the authorised authorities. Twice a year, the Interception Commissioner submits a report to the Prime Minister that is presented to Parliament.[41] This report covers whether the Secretaries of State and public authorities operating under the UK's legal framework regulating surveillance, the Regulation of Investigatory Powers Act 2000 (RIPA)[42], are doing so lawfully.[43]

The report focuses on the interception of communications and requests to access communications data as well as the interception of communications in prisons. Issues covered in the report include the number of requests the authorised authorities have made in the year, how the inspection regime works, findings from the inspections including issues and recommendations for improvement and details of the authorities and public bodies authorised to make requests. Commentary on the adoption of recommendations made in previous years is included as well.

In addition, the Chief Surveillance Commissioner (CSC) oversees how law enforcement agencies use covert surveillance powers and covert human intelligence sources under RIPA Part II and the Police Act 1997. The Intelligence Services Commissioner (ISCom) oversees how the intelligence agencies use the powers available to them under RIPA Part II and the Intelligence Services Act 1994.

The reports by David Anderson, the ISC and RUSI all recommended that this oversight regime needed overhauling, and that three separate oversight bodies with different identities yet overlapping responsibilities was confusing.

The UK draft Investigatory Powers Bill proposes these three commissioners are replaced with one new Investigatory Powers Commissioner (IPC), a senior judge appointed by the Prime Minister. The draft proposes that the IPC's office would be responsible for approving interception warrants, overseeing and inspecting the use of powers under the draft Bill and publishing findings in an annual report, and will have the power to inform individuals who have been subjected to surveillance in error.[44]

[40] http://www.iocco-uk.info/
[41] The Interception of Communications Commissioner Office, Annual Reports (June 2015)
[42] The Regulatory Investigatory Powers Act (RIPA) of 2000 is a key piece of legislation governing surveillance in the UK. Part 1 of the Act (which deals both with interception and communications data) is currently undergoing review.
[43] See the most recent report, covering the period January to December 2014, published March 2015.
[44] See, Draft Investigatory Powers Bill (November 2015) Context, Oversight (P6-7) and Draft Investigatory Powers Bill Factsheet- Oversight (November 2015)

Country Example: Illustrating Aspects of Oversight Models – USA

The Privacy and Civil Liberties Oversight Board (PCLOB) [45] is an independent US Government agency within the Executive branch that was established in 2007 but came to prominence following public revelations of surveillance practices in 2013. Its remit is twofold:

i. To review actions the Executive branch takes relating to terrorism with a view to the consideration given to privacy and civil liberties; and

ii. To ensure privacy and civil liberties are considered appropriately in the development of the legal framework that sets out the steps that can be taken to protect the US from terrorism. The Board has a staff of four and five Board members. Twice a year a report is produced outlining the work of the Board and its findings.[46] Since 2013, the Board has conducted detailed analysis on:
   - Section 702 of the Foreign Intelligence Surveillance Act (which targets communications of non-US persons based outside the U.S),[47]
   - Section 215 of the US Patriot Act (which is used to order companies to hand over phone records and had been used to collect bulk phone records[48]). The PCLOB concluded, *"We have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack."* [49] Section 215 has since been amended in the US Freedom Act to restrict the bulk collection of phone records by US intelligence agencies.
   - Workings of the Foreign Intelligence Surveillance Court (which approves applications for surveillance),
   - Executive Order 12333, enacted during the Regan administration and amended during the George W. Bush administration, that extended the powers of US intelligence agencies.

4. Notification of Individuals Under Surveillance

- It is understood that there will be times when individuals cannot be notified by authorities that they are under surveillance as doing so could jeopardise the surveillance itself.
- However, notification of individuals if they have been the subjects of surveillance is important, and individuals who may have been subject to illegal surveillance should be ensured access to effective remedy**.** At a minimum, users should be notified that

[45] https://www.pclob.gov/
[46] See the latest report (October 2014-March 2015) here: www.pclob.gov/library.html#semiannualreports
[47] Section 702, Foreign Intelligence Surveillance Act.
[48] https://www.eff.org/foia/section-215-usa-patriot-act
[49] Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (23 January 2014) p150.

their communications have been subject to surveillance when the surveillance is complete.
- The legal framework should set out the circumstances under which there may be a delay in individuals being notified that they are under surveillance.

5. Remedy

- Individuals need to know whether they have been subject to surveillance in order to bring a complaint and seek access to remedy. When individuals are informed that they have been subjects of surveillance they should also be informed of the procedure for filing complaints if they wish to do so.
- Any alleged violation of the law – whether on procedural or substantive grounds must be promptly, thoroughly and impartially investigated.
- Where a violation is identified it must be possible to end it. For example, the official body examining a potential violation must be able to order the termination of the surveillance and the deletion of data and the prohibition of its use by issuing binding orders.

6. Transparency

- The legal framework on communications surveillance must be publicly accessible and set out the nature, scope and time-frame of possible surveillance, the requirements that must be met for surveillance to be authorised and which authorities are responsible for authorisation, carrying out and supervising the surveillance.
- There should be a clear explanation of each different type of surveillance that is possible.
- Further, the legal framework should define the circumstances in which there can be sharing of information across borders between governments.
- Publicly accessible information about surveillance set out in the law must be sufficiently clear and precise for individuals to be able to understand it and foresee how the law might be applied to them.
- The process of providing remedy for individuals who have been the subject of inappropriate surveillance must be explained.
- To promote government accountability, authorities should produce as a minimum, the aggregate yearly figures on the specific number of requests for surveillance made, including the number accepted and rejected, details on the way in which such powers are used and information broken down by specific legal authority for example, wiretaps, the number of requests to service providers, etc.

Country Example – Transparency

In 2013 at the direction of the President of the United States, a tumblr account was created (it is maintained by the Office of the Director of National Intelligence) to give direct access to information about the foreign surveillance activities of the US Intelligence Community.[50] This account has details of declassified documents related to intelligence activities, the budget of the intelligence community, and a transparency report detailing the number of requests made using national security legal authorities including FISA and National Security Letters.

7. Provisions for Periodic Review of the Lawful Interception Framework

- Given the speed at which technology develops, and the potential for communications surveillance to infringe rights, it is important that the legislative or regulatory framework includes provisions for periodic review of the law to ensure rights are protected.

The Role of Companies (Communication Service Providers) Providing Communication Service to Users

- Communication service providers should not be compelled to modify their infrastructure to enable direct surveillance that eliminates the opportunity for judicial oversight.
- Any request to service providers for access to communications content or data should be provided in writing, explaining the legal basis for the request including the Requesting Authority and the name, title and signature of the authorised official within the Requesting Authority making the request. Although it is preferred for requests to be provided in writing it is recognised that there are often certain exceptions provided for by law, for example emergency situations and immediate risk to life where oral requests are acceptable, providing they are followed up in writing.[51]
- Service providers should have the right to seek clarification or modification to a request, which does not appear to follow domestic legal procedures or internationally accepted human rights protections.

[50] The tumblr account can be accessed at http://icontherecord.tumblr.com/
[51] See Global Network Initiative (GNI) Principles on Freedom of Expression and Privacy

On-going Debates on Communications Surveillance

Active and on-going debates on communications surveillance show no sign of abating. As noted above, this issue has been the dominant one in the ICT and human rights space. It is therefore likely that there will be a need to update the Model to take account of evolving understandings.

The most important on-going debates are flagged below.

Mass surveillance

As noted above, there is no international agreement on what the term "mass surveillance" means. It refers broadly 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. At the UN level there is serious concern about communications surveillance that is authorised on such a broad and indiscriminate basis because it runs counter to the whole core concept of the protection of privacy that requires justification for intrusions to be made on a case-by-case basis. 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".*[52]

Level of Protection of Communications Data

Surveillance that captures communications data means it is possible to identify the location of the user. This has resulted in questions as to whether the lower level of protection that is given to communications is still appropriate. There are often stronger legal protections requiring a higher burden of proof around the authorisation of lawful interception than for accessing communications data, as it is more intrusive to personal privacy. For example, in the UK there is an important distinction between communications data and content, governed by two separate authorisation regimes. Law enforcement agencies and other government agencies can often obtain communication data through self-authorisation dependent on internal checks and balances. However, access to the content of communications requires authorisation in the form of a warrant signed by the Secretary of State.

[52] UN General Assembly A/69/397 (23 September 2014).

The Protection of Non-Nationals

The issue of whether nationals of a particular country should enjoy higher protections than non-nationals is another topic of current debate. The International Covenant on Civil and Political Rights (ICCPR) by its terms provides protection to all without distinction based on nationality, however some countries interpret the ICCPR in such a way as to give greater protection to their own nationals.

Extraterritorial Reach of Surveillance

Laws that authorise extra-territorial surveillance or the interception of communications in foreign jurisdictions are problematic. These issues were set out in April 2013 by the UN Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion in his report to the UN Human Rights Council.[53]

The short case study on Tunisia below is an example of a country transitioning from a surveillance state to one that better seeks to balance freedom of expression and privacy. Importantly, these rights are underpinned by Constitutional guarantees. The changes made to date are technical, rather than being achieved through legislative reform. The current approach represents a practical and innovative interim technical fix that could provide a useful example to other regulators and prompt a wider debate on approaches to ensuring respect for rights in the digital era. That debate should consider short-term and long-term considerations. On a longer-term basis, a rights-respecting regime enshrined in national law will provide a more secure basis for ensuring that important constitutional and human rights are respected.

Country Example: Other Options to Address Communications Surveillance – Tunisia

Under the former regime, Tunisia was a "surveillance state". Civil society groups had long reported on the strict censorship and extensive monitoring of online communications. After the 2011 revolution, which removed the President from power, the scale of surveillance that had been taking place was revealed.[54] There was a very strong desire from different stakeholders in society to change this and dismantle the surveillance apparatus that existed for decades.[55]

The new Tunisian Constitution now enshrines freedom of the media and freedom of expression in general terms. However there is no new law or amendments to the existing legal framework safeguarding free expression and privacy.[56] Rather than focusing on changes to the legal system and regulatory framework in Tunisia after the revolution, the emphasis was placed on making technical changes to the way in which the Internet worked and moving from heavy censorship and surveillance to a

[53] See the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40 (17 April 2013), p17.
[54] Nancy Messieh, "Tunisian government got discounts on surveillance software in exchange for bug-tracking", *TNW News* (4 October 2011).
[55] Trevor Timm and Jillian C. York, "Surveillance Inc: How Western Tech Firms Are Helping Arab Dictators" *The Atlantic* (6 March 2012).
[56] ARTICLE 19, "Tunisia: Background Paper on Internet Regulation" (July 2013).

free Internet. Prior to the revolution the Tunisian Internet Co. - ATI (former Tunisian Internet Agency) - was the central routing point for the Internet, which made it easier to monitor online communications, censor content or shut down the Internet altogether. Internet traffic is now routed through a variety of different points and exchanges which increases the resilience of the network and also makes it more difficult to censor. There was a focused effort from Internet actors, civil society and the operators to make this change happen, which was initiated by the ATI.[57] This move by the ATI played a critical role in rebuilding trust in the organisation that had played a key role in surveillance and censorship under the previous regime. In 2014, a Decree enshrined the role of the ATI as one of a number of ISPs in Tunisia, removing its previously unique role as the sole router of Internet traffic in the country.

There has not always been government support for this approach in the post revolutionary period. There have been unsuccessful challenges in the courts to reinstate censorship and a proposed law in 2013 on cyber-criminality was withdrawn when the draft was leaked and became public. A strong civil society and public support for a free Internet have played an important role in maintaining this commitment to free expression and privacy in the post revolutionary period.

[57] Yasmine Ryan, "Transforming Tunisia's Internet Agency", Aljazeera (5 October 2011)

Conclusion

Since the revelations of mass surveillance by government agencies that began in June 2013, issues relating to business and human rights in the technology sector, particularly concerning the right to privacy and free expression, have been front-page news around the world. But it is often a difficult debate to follow, with complicated terminology, difficult legal frameworks to understand, much secrecy because of national security considerations and highly technical issues that need to be understood. This Occasional Paper has set out the issues and challenges in a non-technical way, referencing many of the reports that have now been presented to the United Nations and laying out a proposed Model covering the key steps that a rights resecting approach requires.

As more and more people around the world conduct more of their lives online and the costs of storing data reduce dramatically, coupled with the tendency for technology to run ahead of legal frameworks, the need to address the requirements of law enforcement and national security concerns while respecting the right to privacy will become an ever more urgent one. This Occasional Paper has put forward an approach to specific issues – including oversight and transparency requirements, the need for independent and competent authorities to authorise surveillance and requirements for adequate training for those involved in requests to ensure appropriate consideration of the privacy implications of government requests. However, there are significant additional issues such as extra-territoriality and mass surveillance where much work remains to be done to build a meaningful consensus between different stakeholder groups that can lead to action. The appointment of the first UN Special Rapporteur on the right to privacy in July 2015 offers a real opportunity to take this vital work forward.

State surveillance practices have dominated debates in the Information and Communication Technology (ICT) and human rights space in recent years. At times, it is not an easy debate to follow; the legal frameworks surrounding surveillance are complicated, as are the concepts of lawful interception and communications data.

The "Rights Respecting Model for Lawful Interception and Government Access to User Data" presented here seeks to set out important principles for each step of developing and implementing a communications surveillance legal framework that protects and respects human rights.

The work to prepare the recommendations set out in this Paper began in response to ongoing developments in Myanmar, one of the fastest growing telecommunications markets in the world. A key part of Myanmar's telecommunications framework governing lawful interception and government access to user data had yet to be finalised, leaving a significant gap in Myanmar's ICT regulatory framework.

While the Model focuses on work from Myanmar, it also reflects lessons learned from a broader set of countries that have faced similar challenges, drawing in particular from examples of the US and the UK. This Paper outlines the challenges and issues at stake and aims to provide further useful information for governments and other stakeholders involved in drafting legislation. The Rights Respecting Model is relevant to any government seeking to put in place or modify its legal framework for lawful interception and government access to user data. This Paper also aims to provide useful information and a description of the challenges for those with an interest in business and human rights and the technology industry but without specific expertise in these issues.

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

Institute for
Human Rights and Business