Legal Studies Research Paper Series

UNIVERSITY OF CAMBRIDGE
Faculty of Law

PAPER NO. 16/2017

MARCH 2017

Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes

Douwe Korff, Ben Wagner, Julia Powles, Renata Avila & Ulf Buermeyer

Further information about the University of Cambridge Faculty of Law Legal Studies Research Paper Series can be found at http://www.law.cam.ac.uk/ssrn/

Global Report – January 2017

Boundaries of Law

Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes

Electronic copy available at: https://ssrn.com/abstract=2894490

Authors:
Prof. Douwe Korff
Dr. Ben Wagner
Dr. Julia Powles
Renata Avila, LL.M.
Dr. Ulf Buermeyer, LL.M.

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit: http://creativecommons.org/licenses/by/4.0/.

This research project was conducted with support from the World Wide Web Foundation. The opinions expressed in this report do not necessarily reflect the views of the World Wide Web Foundation.

The report is based on data collected until December 2015. There have been changes in some of the countries surveyed during 2016, in particular in the UK and Germany. Which could not be reflected within this report.

Table of Contents

Executive Summary

Modern information technologies have given governments an unprecedented ability to monitor our communications. This capability can be used to fight terrorism and serious crime through targeted surveillance that is proportionate and subject to judicial control. What we have witnessed, however—as evidenced by the revelations of whistleblower Edward Snowden—is exponential growth in indiscriminate, generalised access to bulk communications and Internet data (often referred to as "mass surveillance").

Why does this matter? Our entire lives are online. We generate and share more information than ever before; information that could be abused in the wrong hands. If not tackled, this untargeted, suspicionless mass surveillance will create a chilling effect on speech, trade, and creativity online, and people will refrain from utilizing the Internet to realise its full potential for economic, social, and democratic progress.

In addition, companies are increasingly called upon by law enforcement and national security agencies to cooperate in investigations, resulting in a loss in consumer confidence and damage to a company's bottom line.

Public opinion has shifted since the Snowden revelations. Now more than ever, we need an informed debate on the role of government surveillance in national security and law enforcement. We need to ensure that such surveillance is accountable and transparent.

Experts surveyed in the 2014 Web Index[1] concluded that 84% of the 86 countries covered lacked even moderately effective oversight and accountability mechanisms to protect Internet users from indiscriminate surveillance. A finding as worrying as this needs to be tested, so we carried out a deeper comparative analysis of a smaller sample of countries: Kenya, DR Congo, South Africa, Colombia, Germany, Myanmar, India, Pakistan, France, Turkey, Egypt, Russia, the United Kingdom and the United States. We conducted interviews and desk research on each jurisdiction to get a better idea of the current state of affairs. We have also tried to analyse intra-country intelligence sharing networks and "clubs", but since much of this occurs without accountability, transparency, or meaningful oversight, there are limits to that analysis.

Key findings

1 Globally, legal surveillance frameworks are ineffectual.

The picture that emerges from our study is a bleak one, confirming the global findings of the 2014 Web Index that the overwhelming majority of countries lack effective checks and balances on mass surveillance powers. Not only are legal surveillance frameworks on "international communications" very weak in the US and the UK, but the laws and practices in many other countries are just as bad, and in some cases, worse. These frameworks are so feeble that they allow governments to interfere arbitrarily with the right to confidentiality of communications of hundreds of millions of people worldwide by collecting data in bulk without proven cause for suspicion.

2 The right to privacy is guaranteed in principle, but not respected in practice.

Ten of the 14 countries surveyed (Colombia, DR Congo, Egypt, Germany, Kenya, Myanmar, Russia, South Africa, Turkey, USA) have a constitution which expressly protects the right to confidentiality of communications. In the other four, that right is protected by the incorporation of international human rights standards into the domestic legal system (UK, France), or it can be read into wider constitutional rights such as "privacy of the home" (Pakistan) or even the "right to life and personal liberty" (India—although the judiciary there is reluctant to be active in that respect). In all countries, the right can be restricted (i.e., the confidentiality of communications can be interfered with), in certain circumstances.

In relation to specific, targeted criminal investigations, these circumstances and formalities are typically contained in the domestic Criminal Procedure Code or equivalent laws. The German CPC, for example, allows for targeted interception in criminal investigations on the basis of a judicial authorisation clearly specifying the target of the surveillance, valid for a limited period, with further safeguards including transparency about the use of such warrants, with the publication of detailed, meaningful statistics. Similar constraints are laid down in the laws of France, Russia, South Africa, the UK and the USA. In Colombia, interception in criminal cases can be ordered by a prosecutor rather than a judge, but is still subject to otherwise similar constraints.

In the DR Congo, India, Kenya, Myanmar, Pakistan, and Turkey, a judicial warrant is not required, but in addition, in these countries, the laws do not contain meaningful substantive or formal constraints on the use of interception powers.

Nevertheless, even in the countries listed above that impose serious substantive and formal constraints on interception in criminal case, these constraints tend to only apply to the interception of the contents of communications, and as detailed below, they are often undermined by loopholes, secret laws, extralegal proceedings and interference with network operators and telecommunications service providers so as to weaken these safeguards in practice.

3 There is even less constraint on access to metadata than on content data.

Even in countries such as Colombia, France, Germany, Russia, South Africa, the UK and the USA, in which interception of communications content is in principle subject to important substantive and formal restrictions, access to so-called "metadata" is subject to much less constraint. (In countries that do not seriously limit interception of communications content, such as DR Congo, India, Kenya, Myanmar, Pakistan and Turkey, access to metadata is, of course, also largely uncontrolled). "Metadata" (in the UK referred to as "communications data") are "data about communications", such as the time, date, and duration of a call, the identity of the parties involved in the call or of the devices used (which are of course often closely linked to specific individuals), and the location of the devices (and thus the location of the parties). In the era of mobile communications, such metadata, particularly location data, can be as revealing as—and sometimes even more revealing than—the content of communications. What is more, by being much more structured than content, metadata are much easier to analyse (i.e. "mine" for relevant information) than content data.

4 "National security" is so broadly defined, it is meaningless.

Our most worrying finding is that vague laws often allow unlimited or barely limited access to both metadata and the content of user communications by law enforcement and/or national security agencies, outside of the normal framework for criminal investigations in the name of "national security".

The Johannesburg Principles on National Security, Freedom of Expression and Access to Information—a

document which was drafted by civil society and endorsed by UN Special Rapporteurs and other international—stresses that the notion of "national security" should be limited to real, immediate threats to the very existence of the state or the democratic order. However, we found that in many countries the concept is stretched to include, for example, the fight against organised crime and the protection of the economic interests of the state (France, Germany), the prevention of incitement to commit [apparently any] offences (India), anything relevant to the country's "international affairs" (USA), or any "national interest" (Kenya). In other cases it is deliberately undefined (UK), or left to the discretion of the authorities (Egypt).

In other countries, without necessarily formally stretching the concept of "national security", these kinds of broad targets are still added to the tasks of the national security (or "intelligence") agencies. This is the case in Myanmar, Pakistan, South Africa and Turkey.

The special laws covering state activities in relation to such "national security" issues and/or the activities of the relevant national security or intelligence agencies typically grant the relevant agencies special powers of interception of communications data (both metadata and content), in particular in relation to "external communications" (i.e., to communications travelling over Internet or other digital communication networks, including mobile networks, that are physically outside the country, or that involve at least one "foreign" party). Not only are such practices discriminatory and contrary to the concept of universal human rights, the distinction between "internal" and "external" communications is also largely meaningless in the digital world. For example, most Internet communications between two parties even in the same country will involve sending data over global ("external") pathways.

The "internal"/"external" distinction also loses much of its meaning in light of the existence of intelligence sharing practices among countries. One participating country's "internal" communications are other countries' "external" communications. When these communications are shared and combined, their provenance becomes irrelevant.

At the same time, the relevant special laws impose fewer procedural safeguards or restrictions on the scope, targets, or duration of the surveillance than are typically imposed on law enforcement agencies acting in "normal" criminal cases. In particular, they often allow the agencies to collect data in bulk, untargeted and without identifying any specific suspects or even people associated with suspects; the Court of Justice of the EU calls this "generic access" to communications data. The power to demand such "generic access" (or carry it out directly), at least to "external" communications, is either expressly allowed or can be read into the law in 13 out of the 14 countries studied. In South Africa, it is not clear from the law whether this is allowed, but the authorities there have nonetheless indiscriminately accessed Internet communications in secret, irrespective of the law.

5 Mass surveillance rarely requires judicial authorisation.

In many countries, mass surveillance does not require judicial authorisation. It can be authorised by the government (Myanmar and Pakistan), a minister (the UK), or the prime minister (France), or the president (USA), senior officials (India), the police, the military and the intelligence services (Colombia, DR Congo, Egypt), or indeed "any authorised agency" (Turkey, in undefined "non-delayable" cases).

In Kenya, Russia, and South Africa a judicial authorisation is required. In all three countries, however, no evidence of any actual crime or plot is required, and "national security" is defined so broadly that the threshold for granting authorisation is very low. As a result, the relevant judges are given such little leeway to reject requests that it cannot be considered effective judicial control in practice.

6 Governments can demand direct access to telecommunications infrastructure through "back doors".

We also concluded that the authorities in almost all countries surveyed can, under their laws, demand that Telecommunications Service Providers (TSPs) and (Mobile or other) Network Operators ([M]NOs) install devices to facilitate interception, and that in essentially all cases this could be interpreted as including "back doors", which grant those authorities direct access to the systems of these providers and operators that can be not be monitored by the companies themselves.

Apart from gaining entry to systems through officially mandated "back doors" under the above laws, intelligence agencies are also increasingly "hacking" into

systems they want to monitor, behind the backs of the providers or operators in question. Snowden has revealed that the NSA (US) and the GCHQ (UK) have done this in relation to several Internet "giants". Other technologically advanced countries, such as Russia and China, are likely to try to do at least the same, and there are some reports to that effect (although such reports are difficult to verify).

7 Laws under which untargeted mass surveillance ("generic access")[2] takes place are secret or opaque.

The rule of law implicitly requires that all legal rules—and certainly all legal rules that allow for interferences with fundamental rights—must be publicly accessible. However, in Colombia, Russia and Pakistan, it would appear that even some laws or other primary rules are kept secret. In many other countries, this appears to be the case with regard to subsidiary rules or guidance on or interpretations of the law. Based on our research and interviews, we believe this is likely to be the case in DR Congo, Egypt, Kenya and Myanmar; and it also quite probably the case that there are such secret rules or guidelines or interpretations in India, South Africa and Turkey. Even in the USA and the UK, the most important rules and guidelines and legal interpretations underpinning surveillance have been kept secret until exposed by Snowden or forced into the open in litigation. The recent French surveillance law, adopted on 1 October 2015, contains a provision that allows for secret decrees by the Conseil d'État to regulate the details of the relevant surveillance. And in Germany, the main intelligence agency, the BND, relied on secret, "creative" interpretations of the law to carry out surveillance which constitutional experts say breaches the law.

There is even less transparency about actual practices. In Colombia, Pakistan, Russia and the UK, the law either expressly prohibits the TSPs and (M)NOs from releasing statistical information on interception, or allows the authorities to prohibit it (or the law can be interpreted in that way) and the absence of such statistics on these countries from the operators' reports available through the TID website suggests that those powers have been used to prevent such publication. The absence of these figures in the operators' information on DR Congo, Egypt and Kenya is also likely to be the result of this having been made clear to the TSPs involved. This may also be the case in India and Turkey, on which statistics are also not provided. As for Myanmar, on which Telenor provides only one odd "historical" datum, it would appear that either the company does not know what use is made of the relevant powers (because interception is done directly, through "back doors" that it cannot monitor), or that it is effectively prevented from publishing the relevant data, even though there is no law prohibiting it.

With regard to France, Germany, Russia and the UK, the authorities themselves do provide some information on the use of their surveillance powers. However, our study shows that the official statistics are either partially omitted and partially blacked out (in the UK), or limited and disputed (in particular in relation to extralegal operations, noted below in Finding 9).

There are also caveats about how meaningful the data released by the Telecom Industry Dialogue companies (TID) or those governments really are stresses in its reports). Figures about numbers of warrants can be misleading. In the UK, one external warrant relating to an undersea cable could relate to data on millions of communications by millions of individuals. This lack of data also extends to intelligence-sharing mechanisms where precious little information is available to the public. The informality and opacity of intelligence-sharing agreements poses considerable challenges to accountability, transparency, and rule of law in the surveillance process.

8 There is a trend toward countries conducting surveillance under semi-permanent states of quasi-emergency.

We also noted that in almost all countries, the authorities are given extremely wide-ranging powers at times of war and national emergencies "threatening the life of the nation" (to use the words of the international human rights treaties). However, we found that this is of only limited relevance to our topic as most of the special laws we have examined do not purport to be limited to times of war or such national emergencies. Rather, the mass surveillance powers are granted in laws that are supposed to apply within the normal constitutional frameworks – yet at the same time, they challenge these frameworks. Thus, laws that would not normally be deemed acceptable are becoming an ingrained part of the permanent legal fabric of the countries surveyed. They are creating a "semi-permanent quasi-emergency" legal framework, not fully in accordance with the normal rules but also not formally seen as emergency law.

Thus, in the USA, the President can declare a "national emergency" and then claim certain exceptional powers otherwise reserved for times of war. Such an emergency was, in fact, declared in response to the "9/11"

attacks—and *this declared state of emergency formally remains in effect. However, the President did not need to rely on a the declared state of emergency to issue Executive Order 12333, which is the main basis for the bulk interception of "international communications", because he had the power to issue that order under the President's "inherent authority" under Article II of the Constitution to conduct foreign intelligence.*

By contrast, following the recent massacre in Paris by Belgian and French jihadists, the President of France has declared the country to be "at war" with the "Islamic State", and is seeking to change the constitution to give the authorities wider, less judicially constrained powers. Changing the constitution rather than relying on a temporary derogation for a defined war or emergency underlines the insidious effects of permanent "special" anti-terrorist laws.

9 An alarming amount of mass surveillance happens illegally anyway.

In many countries mass surveillance was conducted outside of the official, known legal framework altogether. Extralegal operations have been revealed in France, Germany and South Africa – and in many other countries: Colombia, Egypt, Kenya, and Pakistan. In Myanmar, Russia, and Turkey the law itself is so unclear as to make it impossible to distinguish between legal and extralegal activities. Up to a point, the programmes of the USA and the UK are also of dubious legality, since they rely so much on secret rules and secret interpretations of the law.

10 Oversight systems are often non-existent or ineffective because they are not independent.

In six of the countries studied there is effectively no independent oversight over the use of the above-mentioned powers of "generic access", not even on paper. This is the case in DR Congo, Egypt, Myanmar, Pakistan, Russia and Turkey. At most, in some of these countries (like Myanmar and Russia), there are internal oversight systems by officials or bodies that are part of the executive branch, but these are, by their very nature, not independent or detached from the system.

In France, the use of the "generic access" powers provided for in the recent law is only subject to "advice" from various bodies rather than real oversight. In India, there is oversight only by a "review committee" made up of high officials, but by law the committee must maintain "utmost secrecy" and destroy its own files after six months.

In countries with generally weak legal systems, such as Colombia and Kenya, oversight regimes are also limited in their real effectiveness. In South Africa, the low threshold for authorisations of surveillance undermines the supervisory function of the "designated" judges that must issue them.

In other countries studied, oversight systems are in place but they have proved to be ineffective. This is in particular the case in the two countries to which the Snowden revelations related most directly—the USA and the UK—but it also applies to Germany, where large surveillance operations, including some carried out with or at the behest of the USA's NSA, were not known to the oversight body, the G10 Commission.

What can be done to improve the current state of affairs?

The discrepancy between continuing government surveillance practices and the relevant international human rights and rule of law standards is breath-taking. The resulting concentration of secret power in the hands of intelligence agencies may prove deeply corrosive to democracy, commerce, and the rule of law. However, in most of the countries studied, citizens and their elected representatives still have the ability to call the State to order and establish appropriate checks and balances on its surveillance powers. Guided by the Necessary and Proportionate Principles, this report proposes a set of standards for minimum transparency, accountability and oversight of government surveillance practices.

Proposed Standards

RULE OF LAW

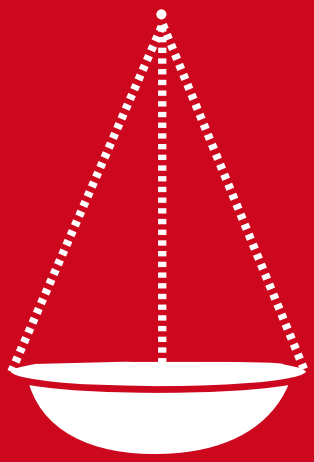
All intelligence and law enforcement agencies should have roles, powers, and responsibilities based on clear, published law, with foreseeable application and effects.

•

Surveillance laws should not allow for activities on the part of intelligence or law enforcement agencies that would violate international human rights law.

•

Surveillance should not allow for suspicionless mass (bulk) collection or retention of any types of data, and should not allow for indiscriminate, "generic" access to data.



TRANSPARENCY AND OVERSIGHT

All intelligence-sharing agreements between and among intelligence and law enforcement agencies - both domestic and international - should be fully public.

•

There should be appropriate public reporting on the exercise of such powers, and of any abuses or deficiencies in the use of such powers.

•

There should be close political, internal administrative and judicial control over intelligence and law enforcement agencies.

•

There should be full, regular ex post facto oversight by a truly independent, technically capable, and fully-empowered supervisory body which avoids capture and ensure technical competence, independent expertise and access to relevant systems.

•

All intelligence and law enforcement oversight bodies should publish a report at least annually on its regular reviews, and should publicly report on any ad hoc inquiry or investigation.

•

Information and statistics in the reports mentioned above should be meaningful and allow real insights. The reports should critically review whether all the actions of the agencies were necessary, proportionate, effective and fair in their own terms and in terms of their outcomes.

ACCOUNTABILITY

Whistleblowers should be strongly protected and whistleblowing mechanisms should be strongly encouraged. Reports on internal and external whistleblowing should be sent to an independent supervisory body. The press and their sources should be protected in their reporting on the activities of the intelligence and law enforcement agencies.

•

When serious wrongdoing is found to have taken place, there should be full civil and criminal liability, in the ordinary courts, without undue protections for the agencies or their staff or their information.

•

Intelligence and law enforcement intelligence sharing practices should be covered by data protection law. Compliance with data protection law should regularly be audited and the results published as part of the annual reporting requirements of the agencies.

1
Introduction, Concepts, Methodology & Case Selection

1.1 Introduction

In 2013, Edward Snowden exposed massive global surveillance programmes by the USA and the UK. Since then, his further revelations as well as information obtained in official inquiries or unearthed by other whistleblowers, journalists, academics, civil society, and the private sector have provided more details about government surveillance, and the exposures are continuing. Despite these efforts, government surveillance practices and the legal frameworks that surround them are not often subject to public scrutiny, and indeed, often deliberately obscured. Most public attention in the past two years has focussed on the revelations about domestic and global surveillance by the USA and the UK, with little focus on the laws and practices of other countries. In this study we have decided to explicitly broaden the focus to include Russia and the Global South in order to help redress this imbalance and to motivate a wider international debate about surveillance regimes.

In order to ensure transparency and accountability of surveillance practices, meaningful information must be made available and subject to rigorous analysis. This report is an attempt to shed some light on surveillance practices by both intelligence services and law enforcement in a range of countries. By taking a more global and comparative view than many existing studies, we hope to provide a broader perspective on whether state practices in this field are, in fact, transparent, accountable, overseen properly, and grounded in law.

We also provide a basic overview of multilateral intelligence sharing agreements insofar as information about these agreements can be gleaned from public materials. While these multilateral agreements are complemented by extensive sets of bilateral arrangements between states, bilateral agreements are beyond the scope of this study. Nevertheless, both types of agreements represent important components of international intelligence sharing which deserve greater awareness and analysis.

Our ambition is to assist in the task of understanding, characterising, and improving laws governing surveillance through analysing and comparing a selective sample of 14 countries through the framework of international law and

human rights. We focus on laws as they appear "on the books", but we also make general remarks on implementation of those laws in the countries concerned and about the transparency about those practices (or lack of it); and we note "extralegal" practices that have been exposed in several countries.

1.2 Terminology

Acronyms

TSP	Telecommunication Service Provider; also referred to as "provider"
(M)NO	(Mobile or other) Network Operator; also referred to as "operator"
LEA	Law Enforcement Agency
NSA	National Security Agency
LI	Lawful Intercept
PI	Privacy International
TID	Telecommunications Industry Dialogue (TID)

In the discussions that have followed the Snowden revelations in many countries and in international fora, reference is often made to **"bulk data collection"** and **"mass surveillance"**, while the Court of Justice of the European Union (CJEU) has coined the term "generic access" to data. Strictly speaking, "bulk data" simply refers to the existence of data in large amounts; the term "bulk data collection" tends to refer to obtaining full access to such large collections, i.e., to all the data held by Internet Service Providers (ISPs) or (Mobile or other) Network Operators ([M]NOs) on the activities of their end-users, or to all the "metadata" they hold, or to the similarly large databases maintained by the "Internet Giants", such as Google, Microsoft, Facebook, etc.

The term "mass surveillance" is used to denote the use of such access to very large datasets, and the "data mining" of them, to carry out "surveillance" over those to whom the data relate, i.e., to keep the people concerned—and the groups to which they may belong—under "close observation".

In its *Safe Harbor* judgment (discussed in section 2.2.2), the CJEU did not use the terms "bulk data" or "mass surveillance". Rather, it referred to *"legislation … [that] authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States..." and referred to "legislation permitting the public authorities [in the USA] to have access on a generalised basis to the content of electronic communications".*

The USA and the UK both strenuously deny that the actions of their national security agencies (in particular, the NSA and GCHQ) revealed by Snowden amount to "mass surveillance". However, the CJEU clearly regards both the obtaining by the authorities of the relevant data in bulk, and the indiscriminate access they have to it, as serious interferences with the rights to privacy and data protection, which are guaranteed in the EU Charter of Fundamental Rights.

In this report, and in particular in our comparative analyses of the various laws in the countries studied (section 2.3), we have focussed on "generic access" to data, of the kind defined by the CJEU. In particular, in sub-section 2.3.4, we assess whether the laws authorise such access, what formalities are imposed on such access, and whether there is meaningful oversight over, and transparency in relation to, the use of such "generic access" powers.

Also in sub-section 2.3.4, we note that the laws in many countries distinguish between communications "**traffic** data" or "**metadata**" on the one hand, and "**content**" of communications on the other, and that the regime for collection of the former tends to be more lax than the regime for collection of the latter. Here, we may already note (as we also again stress

in that sub-section) that such a distinction is difficult to make in practice. Metadata can be as revealing as—and sometimes more revealing than—the contents of communications (and therefore should not be subject to lesser protection); and that automatic analysis and aggregation of metadata is often significantly easier to accomplish than content parsing.

1.3 Methodology

1.3.1 Country Selection

Our comparative analysis is based on a diverse selection of 14 country cases from five different continents: **Colombia, DR Congo, Egypt, France, Germany, India, Kenya, Myanmar, Pakistan, Russia, South Africa, Turkey, United Kingdom,** and the **United States of America.** The intention is to provide a globally inclusive, albeit selective, comparative perspective on surveillance regimes, in order to ensure that any conclusions drawn are not limited to any one region, legal system, political or economic system, or historical context.

Although a primary objective of the study was to be globally inclusive, and in particular to include the global South, the analysis also necessarily included three Western European countries (the United Kingdom, France, and Germany), Russia and the United States, as these countries provide essential context, both historical and contemporary. The United Kingdom, on the one hand, and France and Germany, on the other, have heavily influenced the two main legal systems of the world— common and civil law, respectively. All three are former colonial powers and have deeply influenced the laws in the neighbouring countries and in their former colonies. Russia, as the central country in the former Soviet Union, has similarly influenced the law in many current and former socialist countries, and continues to maintain close links with them.

Intriguingly, when former colonies gained independence, they often still retained the (repressive) emergency and anti-terrorist laws of their former colonisers. In relation to more recent surveillance laws, the Snowden materials show that there is significant "technical-legal assistance" provided by US and UK security agencies' lawyers to governments drafting such laws in countries with which they are allied (not just in the "Five Eyes" arrangement, but also in other NATO countries). It is reasonable to assume that similar cooperation is in place in other intelligence "clubs". One can therefore discern "families" of such laws with similar features.

The resulting comparative overview provides a broad globally inclusive picture of surveillance practices as well as commonalities and differences between these laws. However, specific findings should not be interpreted as necessarily proportionate to what we might find on a global level. We cannot claim that our selection is representative in that sense.

In the chart on page 17, we indicate (in green) the ranking of the selected countries on the World Wide Web Foundation's Web Index; the countries' per capita GDP (in blue); and the character of their legal systems: civil law, common law, and Islamic law (indicated by lines; when there are lines linked to more than one such system, this means the legal system in the country concerned is hybrid, showing elements of two, and in one case three, of these main systems).

1.3.2 Methodology and Sources

a. Comparative legal analysis

We assessed the selected countries according to a comparative legal framework, focussing on the following research objectives in order to better understand:

- whether communications privacy is recognised as a fundamental right in the domestic legal system;
- powers of targeted lawful intercepts (LI) of communications by law enforcement agencies in ordinary criminal cases;
- powers of untargeted "generic access" to communications data by law enforcement and/or national security agencies in relation to terrorism and/or national security;
- special powers in cases of national emergency;
- oversight over the use of the powers; and
- publication of laws and of aggregate data on the use of the powers.

It was not possible within the scope of this short study to carry out comprehensive primary research into the laws of the selected countries. Nor are there any readily available, reliable comparative data sources of government surveillance regimes across the world. The most reliable and consistently comparable (though still limited) published data we drew on was contained in the "Country Legal Frameworks" published by the Telecommunications Industry Dialogue (TID).[3]

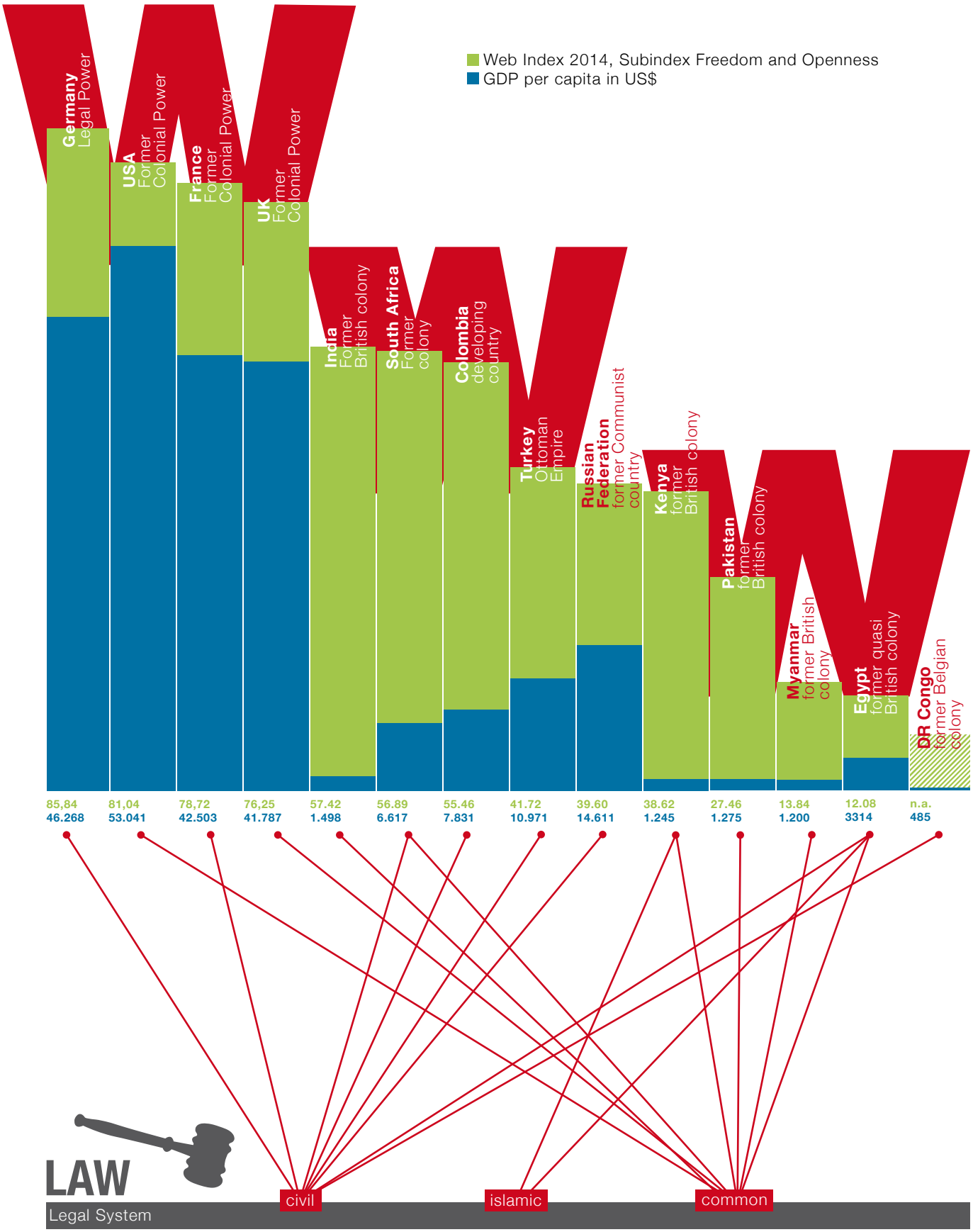
Broader information and context on the surveillance situation in the selected countries was gleaned from country reports by Privacy International (PI) where such existed, and in relation to the USA, from an extensive civil society analysis submitted (like several of PI's reports) to the UN Human Rights Council in connection with Universal Periodic Reviews (UPRs) carried out by that body into the status of human rights in the UN Member States.[4] We also used data from the Web Index of the World Wide Web Foundation to categorise the current Internet policy landscape in the respective countries. Finally, we conducted 29 interviews with industry representatives, civil society actors, and technologists to better ascertain the actual implementation of government surveillance on the ground. Thus the original research here provides a novel perspective on government surveillance from a globally inclusive perspective.

b. Data sharing arrangements

Separately we have attempted to provide an overview of multilateral intelligence sharing agreements between countries that are believed to be in place for both law enforcement and intelligence services. We believe that it is important to obtain some insight into these arrangements, and to increase public debate about them to ensure that citizens across the world know not just who can collect their data, but also how it can be shared and distributed. This research, however, was severely limited by the extreme secrecy surrounding these agreements and the relevant data sharing "clubs". All we can do in this report is highlight the issues, and call for more research and more openness in this regard.

In future, this openness and research should also extend to the question of data sharing between law enforcement agencies and national security agencies both within a single country and across borders. In this report, we merely note the critical comments on that aspect of a proposed new EU-USA law enforcement data sharing "umbrella" agreement. But this, too, is an area into which further research is urgently needed, given the ever-closer cooperation between law enforcement and national security agencies, particularly in relation to the fight against terrorism.

1.3.3 Rankings of Selected Countries with Their Legal Systems



2 Surveillance and Accountability Frameworks

2.1 Introduction

In this section of the report, we analyse international and national laws and practices relating to surveillance. This analysis requires proper contextualisation. The global surveillance programmes that have come under increased scrutiny following the revelations of Edward Snowden are themselves part of a wider trend. This trend increasingly blurs the lines between national security and law enforcement, and blurs distinctions between the agencies relating to these areas at both national and international levels.

One reason for the massive, global increase in broad surveillance practices in recent decades, and especially since September 11, 2001, is a shift in the focus of national security agencies. These agencies have transitioned from countering known foreign state enemies in times of war or quasi-war, to trying to deal with much more diffuse and insidious threats from non-state actors (or at least not officially state-backed actors) in terrorist and "asymmetric warfare" contexts.

The origins of intelligence agencies in Western democracies can be traced back to World War I, but they gained much of their current form during World War II, and remained active behind the scenes during the Cold War. This led to the existence of secrecy beyond the law:

In all secret service activities, which are handled by the central government, the operations of spies, saboteurs and secret agents generally are regarded as outside the scope of national and international law. They are therefore anathema to all accepted standards of conduct.[5]

During World War II, states also began to create international legal and practical frameworks that persist today. For the West, this started with the posting of intelligence liaison officers by the UK and the USA with their respective counterparts during the war, leading to the more formal UKUSA Treaty of 1946 and its gradual expansion to the current Five Eyes states: the UK, the USA, Australia, Canada, and New Zealand. Collaboration continued with the creation of "intelligence clubs" and the close links between the British secret services and the secret services of the newly independent former British colonies, which will be discussed in section 3 in greater detail.[6]

After World War II, the three Western occupation powers granted themselves surveillance rights over the Federal Republic of Germany. After German independence, France, UK, and USA effectively retained these rights and/or obtained full and close cooperation from the intelligence services of the Federal Republic of Germany.[7] The Soviet Union is likely to have granted itself similar privileges in the German Democratic Republic and its other Eastern European satellites, but related documentation has been scarcer.

The conclusion of the Cold War and the rise of non-state global terrorism have changed the role of the agencies, as well as the role of intelligence clubs. Increasingly, intelligence agencies are working closely with the law enforcement agencies in their home country.[8] A further driver for increased surveillance has been the vastly increased technical capabilities for surveillance and data analysis, alongside a dramatic fall in the cost of data collection, storage, and analysis.[9] At the same time, law enforcement agencies are increasingly given powers and roles that were previously reserved for intelligence agencies, especially in the fight against terrorism and other even less-defined threats against national security. In particular, law enforcement agencies are increasingly tasked with the *prevention* of terrorism or extremism, and in the collection of intelligence on a wider array of targets and activities.

2.2 International legal and practical arrangements

2.2. International human rights law: Judicial and political demands for compliance

2.2.1 Basic human rights principles

All international human rights bodies and fora agree on the basic approach to be taken in any assessment of whether certain interferences with fundamental rights are compatible with the treaties that protect those rights. In particular, there is close convergence in this regard between the approach of the body guarding the main global human rights treaty, the International Covenant on Civil and Political Rights (ICCPR), the **Human Rights Committee** (hereafter: the Committee), the court upholding the European Convention on Human Rights (ECHR), the **European Court of Human Rights** (ECtHR), and the court applying the EU Charter of Fundamental Rights (EU CFR), **the Court of Justice of the EU** (CJEU).[10]

But the same approach is also essentially adopted by the **Inter-American Commission and Court of Human Rights** overseeing the implementation of the American Convention on Human Rights (ACHR)[11] and the **African Court on Human and Peoples' Rights**, which assesses compliance with the African Charter on Human and Peoples' Rights.[12]

Essentially, all these treaties, as interpreted and applied by all these judicial and quasi-judicial treaty bodies, require the following:

- Any interference (a term that includes anything that has an impact on protected rights, including any formalities, conditions, restrictions or penalties) must be based on a "law" that meets certain "quality" requirements. The relevant legal rules must be clear, specific

and, above all, accessible (published) and foreseeable in their application. More specifically, the law must protect against arbitrary use of interference powers, such as may occur if the law is excessively vague and/or places excessive discretion in the hands of those authorising or exercising the relevant power.

- Interferences with fundamental rights must serve a legitimate aim in a state under the rule of law (the ECHR says "in a democratic society"). The human rights treaties all recognise that national security, public safety, and the prevention of disorder or crime constitute such legitimate aims.
- No interference with a fundamental right is permissible under the treaties if it compromises the very essence of the right – which as we shall see is relevant in the present context.
- Interferences that respect the essence of a right must still be "necessary" to protect the legitimate interest in question; and for a measure that interferes with a right to be "necessary", it has to correspond to a "pressing social need", and it must be "proportionate" to that need. (The Inter-American jurisprudence tends to use the term "adequate", but the tests remain essentially the same.)
- The proportionality principle can be understood as comprising a "least intrusive means" or "least onerous means" test – meaning that if a state interferes with a fundamental human right, it must choose the least intrusive means that are still capable of achieving the relevant legitimate objective.[13]
- Anyone whose rights have been interfered with in a way that allegedly violates the above must be provided with an effective remedy against the alleged violation.
- There must be no discrimination in the enjoyment of the right.

This approach also underpins the International Principles on the Application of Human Rights to Communications Surveillance (also called the "Necessary and Proportionate Principles") developed by civil society in relation to surveillance.

2.2.2 The Basic Principles Applied to Surveillance

The globally accepted basic human rights principles outlined above have been applied most specifically to surveillance by the European Court of Human Rights in a series of cases going back many years; and more recently also by the Court of Justice of the EU, in relation to more specific issues such as compulsory suspicionless retention of communication data and "generic access" to data on EU persons by state authorities in the USA.

ECtHR case law[14]

The case law of the ECtHR shows the following considerations and requirements of European human rights law relating to surveillance:

- A system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it.
- The mere existence of legislation supporting the secret monitoring of communications entails a threat of mass surveillance.
- In view of these risks, there must be adequate and effective guarantees against abuse of surveillance powers.
- Effective guarantees include that surveillance powers must be set out

in statute, or primary law, rather than in subsidiary rules, orders or manuals. The rules must be in a form open to public scrutiny and knowledge. Secret, unpublished rules are fundamentally contrary to the rule of law and the European Convention on Human Rights.

Furthermore, the ECtHR requires the following "minimum safeguards" to be provided for in published laws on surveillance:

- offences and activities warranting surveillance should be clearly and precisely stated;
- categories of people that may be subjected to surveillance should be stated;
- strict limits on the duration of any ordered surveillance must be set;
- strict procedures for ordering the examination, use, and storage of data obtained through surveillance must be followed;
- strong safeguards against abuse of surveillance powers, including strict purpose and use limitations (e.g., preventing easy disclosure of intelligence data for criminal law purposes) and strict limitations and rules on when data can be disclosed by national security agencies (NSAs) to law enforcement agencies (LEAs), etc., must be provided;
- strict rules on the destruction/erasure of surveillance data must be established to prevent surveillance from remaining hidden after the fact;
- persons who have been subjected to surveillance should be informed of this as soon as it is possible without endangering national security or criminal investigations, so that they can exercise their right to an effective remedy, at least after the fact; and
- bodies charged with supervising the use of surveillance powers should be independent and responsible to, and be appointed by, Parliament rather than the executive branch.

Under the ECHR, these principles must be applied to anyone who is affected by surveillance measures taken by any Council of Europe member state. In addition, European states have a "positive obligation" to protect their citizens from surveillance contrary to the above, perpetrated by any other State. They are under a legal obligation not to actively support, participate, or collude in such surveillance by a non-European state.

The above principles were clearly and strongly re-affirmed in the very recent ECtHR judgment, *Roman Zakharov v. Russia*.[15] Further clarification of the law is expected in the pending case *Big Brother Watch, Open Rights Group, English PEN and Kurz v. the United Kingdom which* specifically deals with the surveillance revealed by Snowden, insofar as carried out by the UK (i.e., by GCHQ).[16]

Case Law of the CJEU

There have been two important recent judgments of the Court of Justice of the EU that have a bearing on the issues addressed in the present report.

The data retention judgment:[17]

Under Directive 2006/24/EC, EU Member States were required to impose on telecommunication service providers in their jurisdiction a duty to retain considerable amounts of so-called "traffic data" (or "metadata") on the communications of the end-users of their services (i.e., on the calling number, the called number, the length of the call, the location from which the call was made, details of the devices used, etc., but not the content of the communications). The directive was challenged, and the High Court of Ireland referred the case to the Court in Luxembourg for a preliminary

ruling. The CJEU held: (i) that the mere compulsory retention of the data in itself constituted an interference with the right to privacy and confidentiality of communications of the end-users (some states had argued that there was only an interference if and when the data were actually accessed by officials); and (ii) that the requirements imposed by the directive were disproportionate to the legitimate aim of preventing crime.

In the latter respect, the Court took into account a range of issues: the application of the data retention duty to all manners of communications, *"entail[ing] an interference with the fundamental rights of practically the entire European population"*; the covering of all persons and all means of electronic communication *"in a generalised manner…without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime";* its application *"even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime"*; the lack of definition of such crimes; the absence of any exceptions to protect professional confidentiality (e.g., of journalists, doctors, lawyers, priests or members of parliament); the absence of any restrictions on compulsory data retention in relation to (i) data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or in relation to (ii) persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences; the absence of any prescribed limits on access to or subsequent use of the data; the failure to provide for any *"prior review carried out by a court or by an independent administrative body".* **Taking all these matters into account, the Court concluded that:**

It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter [guaranteeing the rights to privacy and data protection, respectively]. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary. (para. 65)

It is notable that the points of criticism in this judgment relate to essentially the same issues as those highlighted in the ECtHR case law. In a way, they are the negative expression of the same points noted in the bullet-points above. The two European courts clearly agree that in assessing the compatibility of surveillance laws with European human rights standards, one should look at the clarity and precision—i.e., the foreseeability—of the law in question; at the scope of the law, in particular at who may be affected by it and whether they are reasonably linked in some way to serious crime, and at any exceptions for journalists, lawyers, etc.; at the restrictions and limitations on access and use of the data; and at procedural safeguards, and the nature and effectiveness of those safeguards.

After assessing the Data Retention Directive in these regards, and in relation to data security, the CJEU held that it failed to comply with the principles of lawfulness, proportionality, and necessity, and was therefore invalid *in toto* and *ab initio.*

The "Safe Harbor" Judgment[18]

An EU citizen, Maximilian Schrems, complained to the Irish High Court that the Irish Data Protection C ommissioner (DPC) had refused to investigate a complaint he had lodged about the transfer of his data by the Internet company Facebook to a server in the USA where, he argued, the data could be indiscriminately accessed by US authorities including the National Security Agency (NSA). The Irish DPC had refused to investigate, on grounds that the transfers of the data had taken place under the so-called "Safe Harbor" Agreement concluded between the EU and the USA, which the EU Commission had declared to provide "adequate safeguards" for such transfers. Just as in the data retention case, the Irish High Court referred the case to the CJEU for a preliminary ruling. The Luxembourg Court ruled that the Commission decision holding that the "Safe Harbor" Agreement ensured "adequate" protection for data transfers to the USA was invalid.

For the present purposes, the most important aspect of the judgment was that the Court reiterated its ruling in the *Data Retention* case: Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail.

In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.

Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. (paras. 93–95, references omitted)

In other words, in terms of the EU Charter of Fundamental Rights, legislation allowing state authorities "generic" and indiscriminate access to the content of communications "compromises" the very "essence" of the right to privacy and confidentiality of communications; and legislation that "does not lay down clear and precise rules" governing access even to metadata, and legislation that does not provide for "effective judicial protection", cannot be necessary or proportionate to the legitimate aims of crime prevention or national security. This constitutes the most precise and specific legal guidance with respect to surveillance in any international forum to date.

As already noted, the European Court of Human Rights will soon have to rule on whether this same approach is also followed by that court.

Views of other international human rights bodies

Other international human rights bodies have not yet been called upon, or taken it upon themselves, to adopt rulings or views on surveillance as specific as the European ones.[19] However, the Human Rights Committee's Concluding Observations on the Fourth Periodic Report of the United States of America clearly echo the above. Specifically, having expressed its concern about the surveillance revealed by Snowden, it held that the USA—and by implication any other State Party to the ICCPR—should:[20]

(a) Ensure that any interference with the right to privacy complies with the principles of legality, proportionality, and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance;
(b) Ensure that any interference with the right to privacy, family, home, or correspondence is authorized by laws that: (i) are publicly accessible; (ii) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (iii) are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance; procedures for the use and storage of data collected; and (iv) provide for effective safeguards against abuse;
(c) Reform the current oversight system of surveillance activities to ensure its effectiveness, including by providing for judicial involvement in the authorization or monitoring of surveillance measures, and considering the establishment of strong and independent oversight mandates with a view to preventing abuses;
(d) Refrain from imposing mandatory retention of data by third parties; and
(e) Ensure that affected persons have access to effective remedies in cases of abuse.

In her report on The Right to Privacy in the Digital Age,[21] **the UN High Commissioner for Human Rights also echoed the above, by calling for:**
further practical guidance, grounded in international human rights law, on the principles of necessity, proportionality and legitimacy in relation to surveillance practices; on measures for effective, independent and impartial oversight; and on remedial measures. Further analysis also would assist business entities in meeting their responsibility to respect human rights, including due diligence and risk management safeguards, as well as on their role in providing effective remedies. (para. 51).

The same goes for an *issue paper* released by the Council of Europe Commissioner for Human Rights on The rule of law on the Internet and in the wider digital world.[22] **It concludes, *inter alia,* that:**
Suspicionless mass retention of communications data is fundamentally contrary to the rule of law, incompatible with core data-protection principles and ineffective. [States] should not resort to it or impose compulsory retention of data by third parties.
[States] should bring the activities of national security and intelligence

agencies within an overarching legal framework. Until there is increased transparency on the rules under which these services operate – domestically, extraterritorially and/or in co-operation with each other – their activities cannot be assumed to be in accordance with the rule of law.

[States] should also ensure that effective democratic oversight over national security services is in place. For effective democratic oversight, a culture of respect for human rights and the rule of law should be promoted, in particular among security service officers. (Conclusions & Recommendations 6, 20 and 21)

Views of International Parliamentary Bodies [23]

In April 2015, following an inquiry and report by its rapporteur, Pieter Omtzigt, the **Parliamentary Assembly of the Council of Europe** also called for a ban on untargeted surveillance, calling for a *"strict prohibition"* on "the creation of *'back doors' or any other techniques to weaken or circumvent security measures or exploit their existing weaknesses"; "adequate judicial and/or parliamentary control mechanisms"* over the intelligence services, including *"the power to review international co-operation without regard to the 'originator control' principle, on a mutual basis"*; a ban on economic and political espionage; a ban on the export of advanced surveillance technology to authoritarian regimes; and the adoption of a multilateral *"intelligence codex"* for the intelligence services.[24]

This was followed, on 21 October 2015, by the adoption by the **Inter-Parliamentary Union** (IPU), which represents parliamentarians from 160 countries, of a strongly worded resolution, *Democracy in the Digital Era and the Threat to Privacy and Individual Freedoms,* which *inter alia* stressed that *"all legislation in the field of surveillance, privacy and personal data must be based on the principles of legitimacy, legality, transparency, proportionality, necessity and the rule of law"*; urged reviews of existing law to ensure this; called for a prohibition of extraterritorial or untargeted bulk data collection; demanded *"strict judicial procedures for the authorization of communications surveillance and to monitor the implementation of those procedures, limits on the duration of surveillance, security and storage of the data collected, and safeguards against abuse"*, and action to prevent *"[by-passing of] privacy protections in national law…by reliance on secretive and informal data-sharing agreements with foreign States or multinationals";* and *"strongly urge[d] parliaments to review and establish effective, independent and impartial oversight mechanisms"* and to investigate any shortcomings in their oversight functions.[25]

On 29 October 2015, the **European Parliament** adopted a resolution "on the electronic mass surveillance of EU citizens" on the basis of an extensive inquiry by its LIBE (Civil Liberties) Committee.[26] In addition to calling for suspension of the EU-US "Safe Harbor" Agreement and Terrorist Finance Tracking Programme and a review of the EU-US Mutual Legal Assistance treaty (MLAT), the resolution reiterated Parliament's call to the US authorities and the EU member states *"to prohibit blanket mass surveillance activities and bulk processing of personal data of citizens", and its denunciation of "the reported actions by intelligence services that have severely affected EU citizens' trust and their fundamental rights".* It drew special attention to the CJEU's Data Retention Directive judgment and its concurrence with ECtHR case law on *"general programmes of surveillance"*; stressed that

"any decision to use surveillance technology should be based on a thorough assessment of necessity and proportionality"; called for the EU to *"contribute to the development of international standards/principles at the UN level, in line with the UN International Covenant on Civil and Political Rights, in order to create a global framework for data protection, including specific limitations with regard to collection for national security purposes"; and warned that "only if credible norms are established at the global level can a 'surveillance arms race' be avoided".*

Views of International Non-governmental Organisations

The standards set out on the previous pages are also strongly supported by **non-governmental organisations all over the world**, who have collectively expressed them in the International Principles on the Application of Human Rights to Communications Surveillance (commonly referred to as *"Necessary and Proportionate Principles"*), endorsed by more than 400 non-governmental organizations and the Global Network Initiative, and also welcomed by the above kinds of fora, including the IPU.[27] The principles specifically turn on the concepts discussed earlier: legality; legitimate aim; necessity; adequacy; proportionality; the need for surveillance authorisations to be made by "a competent judicial authority that is impartial and independent"; due process; user notification; transparency; public oversight; integrity of communications and systems; safeguards for international cooperation; safeguards against illegitimate access; and a right to an effective remedy. The principles themselves briefly expand on each of these, with more technical/legal analyses underpinning each of them provided in a separate document.

Conclusions

In sum, there is a clear groundswell of opinion—judicial and political—in favour of tight restrictions on, and effective oversight over, surveillance activities of national security agencies, and on and over their (to date, largely secret) transnational cooperation arrangements. The basic legal framework for this is becoming clear, in particular in the case law of the European courts, but with guidance and recommendations from additional global fora. In the next section, we will examine the national laws in the light of these increasingly established principles.

2.3. National legal and practical arrangements – A comparative analysis

2.3.1 What is being compared

In this section, we look at how interception of communications and wider surveillance over digital communications are regulated in the countries studied. We first, at 2.3.2, briefly look at the constitutional protections accorded to the right to confidentiality of communications. We then, at 2.3.3, describe the "typical" or normal legal framework for interception in relation to "ordinary" criminal investigations by law enforcement agencies, with reference to the **German** system by way of illustration. Only then, in 2.3.4, do we come to the main topic of this report: broader, "mass" or "bulk" surveillance in the kinds of programmes exposed by Edward Snowden as being carried out by the **USA** and **UK** national security agencies.

It would be wrong to assume, however, that one can draw clear delineations here, and in particular that one can clearly distinguish between "normal" powers of the ordinary law enforcement agencies (LEAs) used in

"normal" criminal investigations and separate, special powers, granted only to national security agencies (NSAs), for use in the gathering of "intelligence" on threats to national security, outside times of war.[28]

This ambiguity is because the distinctions between "ordinary" criminal law and "threats to national security" are increasingly blurred, particularly in relation to terrorism, and because, with that, so are the distinctions between the mandates given to law enforcement agencies and national security agencies, and indeed between the agencies themselves.[29] "Terrorism", which is itself an ill-defined term, in inseparably entangled with other forms of serious, organised, transnational crime, including online criminal activities and money laundering. "Cybercrime" and "cybersecurity" are increasingly regarded as matters of national security (in particular in relation to critical national infrastructure). In relation to such matters, the law enforcement agencies are becoming increasingly pro-active and focussed on prevention rather than *ex post facto* apprehension of criminals, i.e., they are increasingly focussing on obtaining "intelligence" on future threats rather than on gathering evidence for apprehension and prosecution of perpetrators of crimes that have been committed. At the same time, the "intelligence"/national security agencies are increasingly assigned a role in tackling relevant "special" crimes: from terrorism and serious cybercrime to online child abuse (and this is even slipping into protection of intellectual property). Indeed, in some countries, the agencies themselves are becoming hybrids, with the dual roles of fighting crime and protecting national security. The **US** Federal Bureau of Investigation (FBI) is a prime example[30] but in the **UK**, too, GCHQ is working increasingly closely with the law enforcement agencies.[31]

As a result, sub-section 2.3.4 is complex, in that it covers overlapping powers by agencies (law enforcement and national security agencies) with increasingly overlapping mandates and shared powers. The complexity is increased by the fact that these overlaps are different in different countries: in some (like **Germany**), a relatively clear distinction continues to be made between the roles and powers of LEAs and those of NSAs. In other countries, new, special powers and special technologies are granted without discrimination between the different agencies. Rather, the powers and technologies are made available to any agency—LEA or NSA —that is involved in stipulated matters (often rather vaguely), e.g., the fight against "terrorism" or "serious organised crime". Finally in sub-sections 2.3.5 and 2.3.6, we will briefly look at the even wider powers that the authorities are granted in times of war or official (declared) "national emergencies" and secret "extralegal" operations.

2.3.2 Constitutional Protections and Exceptions

Ten of the 14 countries surveyed (Colombia, DR Congo, Egypt, Germany, Kenya, Myanmar, Russia, South Africa, Turkey, USA) expressly protect the right to confidentiality of communications in their constitutions, usually in the same article as the one that guarantees respect for the home and/or private life.[32] But all countries also either expressly clarify that the right can be limited by law or by court order; or this possibility of imposing legal limitations is inherent in the constitutional legal system of the country. One **(South Africa)** specifically clarifies in its constitution that the right is not "non-derogable" in times of emergency, but that is generally also the case in the other countries.

Strong legal protection of confidentiality of communications, however, does not necessarily require an express constitutional guarantee. In **France**, the Constitution cross-refers to the 1789 Declaration of Human Rights which does not contain a right to privacy or private life or confidentiality of communications—but the right is given essentially equal protection with other rights through the Civil Code and the Code on the Mail and Electronic Communications, and through the application of the European Convention on Human Rights in domestic law. In the **UK**, where there is no written constitution, these rights are protected under the Human Rights Act, which similarly gives domestic legal effect to the ECHR. And in **India** and **Pakistan**, the right can be read into other rights such as "privacy of the home" (Pakistan) or even the "right to life and personal liberty" (India – although the judiciary there is reluctant to be too active in that respect).

The Fourth Amendment to the Constitution of the **USA** protects against "unreasonable search" but is quite extensively interpreted as providing protection also of communications. However, this protection is limited to US nationals and lawful US residents (so-called "US persons") and does not extend to "non-US persons".[33]

2.3.3 Targeted lawful intercepts by law enforcement agencies

a. The normal criminal procedure system

In most developed legal systems under the rule of law, "normal" communication interception ("lawful intercept") by the normal law enforcement agencies in the course of ordinary criminal investigations (i.e., not related to terrorism or national security) is provided for under the normal law on police investigations and pre-trial criminal investigations[34]; and intercepts regulated quite strictly.[35] Below, we will provide an illustration of such "typical", "normal" rules with reference to **Germany**. However, we also note, at c), that even in normal cases, there are certain exceptions and contradictory approaches to these rules, also in **Germany**.

We will look at the laws applying to non-"normal" cases at 2.3.4, below, where we shall see that they often depart much more seriously from the normal rules.

b. Illustration

This normally strict regulation is well reflected in the typical **French** and **German** Criminal Procedure Codes (respectively, the *Code de Procedure Pénal*, CPP, and the *Strafprozeßordnung* or StPO). To use the latter as illustration, the **German** StPO stipulates that telecommunications may only be "monitored and recorded" without the knowledge of the person concerned if the following conditions are met:

- specific facts justify the suspicion that someone is involved in a serious criminal offence (as listed in §100a(2) StPO) or in the preparation of such an offence by criminal means;
- the specific act is also serious in the specific case; and
- the establishing of the facts or of the location of the suspect by other means would be considerably more difficult or unachievable. (§100a (1) StPO)

The StPO furthermore stipulates that the Lawful Intercept Order may only be issued against the suspect or against other persons "with regard to whom it may be assumed, on the basis of specific facts, that they ac-

cept or pass on messages on behalf of the suspect or which come from the suspect, or that the suspect uses their connection." (§100a(3) StPO). Moreover, an intercept is not allowed if it is likely that it will only result in the collection of "information about the essence of [the surveilled person's] private life". If such highly intimate information is accidentally collected, it must be immediately erased, with a formal note made in the file about the obtaining and deletion of the data (§100a (4) StPO).

In addition, there are crucial procedural safeguards. Thus, a Lawful Intercept Order may only be issued by a court at the request of the public prosecutor, except in urgent cases when the prosecutor[36] may issue the order, but in that case the order must be confirmed by the court within three days. The order must be in writing, with details about the devices to be monitored. It can be valid for no more than three months, but is renewable on the same conditions as before (§100b (1) and (2) StPO).

Telecommunication service providers (TSPs) are required to cooperate with the implementation of the order (§100b (3) StPO). The technical details for this cooperation are determined in accordance with the Telecommunications Law and the Telecommunications Interception Regulation. The interception must cease as soon as one of the conditions listed above is no longer met; and the court must then be informed about the results of the interception (§100b (4) StPO). Finally, the state (Land-) and federal authorities responsible must provide the following details to the Ministry of Justice annually, which the Ministry must publish on its website:[37]

- the number of criminal cases in which Lawful Intercept Orders were issued;
- the number of such orders issued, with detail as to whether they were original orders or continuation orders; and as to whether they related to landline, mobile, or Internet communications; and
- the crime under investigation, in relation to which the orders were issued.

Individuals must furthermore be informed of the interception and monitoring when it has ended (unless this endangers overriding interest), and can challenge the legality of the measures and obtain compensation (as well as erasure of recorded information) if the measures were unlawful (which includes both formal illegality and disproportionality).

The German framework for ordinary, non-terrorist/national security cases is a good example of legal arrangements clearly meeting the constitutional and international human rights requirements in terms of substance (limiting interception and monitoring to specified serious cases and to persons directly linked to a case under investigation, as demonstrated by objective "specific" facts); in terms of process (judicial authorisation, in principle ex ante, and ex post facto only when clearly necessary); limitations (no monitoring or recording of particularly intimate information); and general transparency (in the form of the above-mentioned statistics).

This "typical" or "normal" system reflects the fundamental principles of legality, necessity and proportionality, as well as those requiring due process, rights and remedies, and transparency and accountability. It clearly constitutes "best practice" in this field.

The **French** Criminal Procedure Code (Art. 100) reflects the same principles contained in the **German** Criminal Procedure Code—and these codes directly inspired codes and laws not only in most of Continental Europe but also in the former French and German colonies.

Many common law countries now also require judicial warrants for lawful interception in "normal" criminal investigation.[38] In the **USA**, this flows from the strong protection of communications nowadays provided under the Fourth Amendment to the Constitution (if one leaves aside the non-applicability of the Fourth Amendment to "non-US persons").

The principle that "normal" lawful intercepts (at least of the content of communication) should be allowed only in certain relatively serious cases, and subject to a court order, is contained also in the laws of such diverse countries as **Russia** and **South Africa.**

However, there are a number of important exceptions to such legislative practice as well as approaches that undermine the above principle.

c. Exceptions and Contrary Approaches

First of all, a judicial order is not required in all the countries surveyed in this report. Thus, the **Colombian** CPC allows for interception to be ordered by the procurator (fiscal). In **Pakistan**, interception of communications is regulated, not in the Criminal Procedure Code or the 2002 Police Order, but in the Pakistan Telecommunication (Re-Organisation) Act 1996 (PTRA) which gives sweeping powers of interception to a wide range of authorities, without the need for judicial warrants or orders. In the **DR Congo, India, Kenya** and **Turkey** as well the law is sweeping and does not require judicial authority for interception. In **Myanmar**, the current framework is unclear to say the least, although regulations on lawful intercept are apparently being drafted. Finally, in the **UK** intercept warrants are issued by a politician, the Home Secretary.[39] A new draft law, introduced while this report was being written, suggests the involvement of a "judicial commissioner", but only in a marginal way. It is too early to assess this proposal, as the end-result may be quite different.[40]

Secondly, even in the countries that were originally standard-setting in these regards, the strong principles illustrated above are often limited in their application. In particular, they relate to access to the contents of communications. Thus, even in **Germany** with its strong basic structure, "line identification" data and other limited data (not amounting to full "metadata") can be obtained on demand in relation to even minor offences by a wide range of authorities (§ 111 TKG).

Many other countries create less graded levels of access, distinguishing primarily between "traffic data" or "metadata" as one category, and "content" as another, in spite of the fact that this distinction is difficult to make in practice.[41] And that "metadata" can be as revealing as—and sometimes more revealing than—the contents of communications. As Edward Felten, the first Chief Technologist at the US Federal Trade Commission, put it, metadata can often be a "proxy for content".[42] In addition, automatic analysis and aggregation of metadata is often significantly easier to accomplish than content parsing.

In **France**, access to metadata can be authorised by either a procurator or a judge (more specifically, the investigative judge *[juge d'instruction]* acting in a criminal investigation), while access to communication content must be ordered by a judge. In **Russia** too, access to metadata does not require a court order, while interception of the content of communication does. In **Egypt**, access to both metadata and content can be ordered by either a procurator or a judge. In the **UK**, even interception of content of commu-

nication does not require a judicial warrant, interception of metadata also does not require one. In fact, access to metadata can be "self-authorised" by a wide range of public bodies. In the US, access by public authorities to metadata is generally unregulated as a result of the so-called "third party" doctrine: the data have been "voluntarily" disclosed to third parties and no longer quality for privacy protection—such as the phone numbers that subscribers automatically provide to a TSP or (M)NO every time they place a call.

Furthermore, in many countries (including the ones mentioned above as having compliant, rule of law frameworks for "normal" lawful interception) broad, "generic access" to communication data (metadata and content) is now often granted in "special" cases under separate, new, less demanding legal rules. Typically, these special cases relate to terrorism or other "national security" matters, but the special powers are extended not only to national security agencies but also to law enforcement agencies.

Moreover, in official (declared) emergencies, there are even fewer restrictions. And finally, there have been revelations about extensive mass interception of communications apparently outside of the law – in clear and disturbing departures from the traditionally strict rules. We will briefly discuss these emergency powers and "extralegal" practices.

2.3.4 Untargeted Generic Access ("Mass Surveillance")

What is generic access?

In this sub-section, we will analyse the laws allowing for access to communication data – be that metadata or content – on a "generic" basis, or, as the CJEU defined it in the *Schrems case:*[43]

[Access authorised by a law] without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail.

The **USA** and the **UK** both strenuously deny that the actions of their national security agencies (in particular, the NSA and GCHQ) revealed by Snowden amount to "mass surveillance". But the Court ruled that they do amount to what it calls "generic access" (as defined above). There is also no longer any doubt that when this generic access relates to the content of communications, it "compromises the essence" of the right to data protection, in violation of the EU Charter of Fundamental Right and hence also probably of similar protections in other human rights treaties.

This sub-section looks at whether such "generic access" is legally allowed, outside times of war and emergency, in the countries surveyed, and under what conditions.

Which agencies are granted generic access powers?

One of our main findings is that, in relation to the fight against "terrorism" and the protection of "national security", the powers of the law enforcement agencies and those of the national security agencies can no longer be disentangled. In almost all the countries surveyed, the powers of "generic access" (as the CJEU called it) can be exercised in relation to terrorism or national security by either LEAs or NSAs (and sometimes other authorities as well), on essentially the same basis.

The main issue is not so much about which agencies can use these powers, but rather, for what purposes can an agency (an LEA or an NSA) use powers of "generic access"; how are those purposes defined; and to what authorisations are they subject. We will look at the relevant conditions below, as well as the related power to demand that the entity that is asked to assist in the obtaining of the information (i.e., the Telecommunication Service Providers [TSPs] and/or the [Mobile or other] Network Providers [(M)NOs]) comply with certain "technical requirements" to facilitate the access. In particular, we examine whether this includes a duty to allow the building in of "back doors" into their systems, through which the surveillance agencies can directly access the data, without further involvement of the TSPs or the (M)NOs, indeed with them possibly being unaware of the extent of the use of the facility.

We discuss the oversight regimes (if any) over the use of the relevant powers, and the existence (if any) and effectiveness of available remedies for individuals affected by the exercise of the powers. Finally, we discuss the transparency, or lack of it, in relation to the use of the powers.

The purposes and types of communication for which generic access can be authorised

Our study indicates that two matters are crucial in relation to "generic access". First of all, it tends to be allowed for investigation of "national security" and "terrorism" threats. And secondly, at least in some countries, it is allowed in relation to "external" or "international" communications, but not in relation to "domestic" or "internal" communications.

National Security and Terrorism

The lines between "national security" and "anti-terrorism" activities and conventional law enforcement are increasingly blurred. In part, this stems from the increasingly broad mandates of the relevant agencies. Thus, in many countries the concept of "national security" includes, for example, the fight against organised crime, or the protection of the economic interests of the state; or is left to the discretion of the authorities (Egypt). In others, these latter targets are added to the tasks of the law enforcement agencies, which are then granted "special" powers of generic interception to carry them out.

Thus, under **US** law (in particular, 50 U.S.C. §1881a, introduced by the Federal Intelligence and Surveillance Act [FISA] Amendment Act), the national security agencies serve "foreign intelligence" purposes which are very widely defined to include not just countering terrorism and other major threats to the state but also gathering information on organised crime, or on [apparently any kind of] foreign-based political organisations, and economic information "of interest" to the state.[44]

In the **UK**, the authorities actually refuse to define "national security" so as to retain "flexibility". In the words of the Court of Appeal, it is a "protean concept",[45] **"designed to encompass the many, varied and (it may be) unpredictable ways in which the security of the nation may best be promoted'.**

In **Egypt**, not dissimilarly but more bluntly, national security is defined at the discretion of the authorities; and in **Kenya**, the Constitution itself stipulates that "national security" covers the protection of any "national interest". The **Russian** President has set out the "National Security Concept of the Russian Federation" in similarly sweeping terms in Presidential Decree No. 24 of 10 January 2000.

In **India**, "national security" is defined in the Information Technology Act and the (older) Indian Telegraph Act and Indian Telegraph Rules so as to include "the prevention of incitement to commit [apparently any] offences".
Such sweeping definitions of national security contravene the *Johannesburg Principles*, developed by the NGO "Article 19" and endorsed by UN Special Rapporteurs and other global and regional fora, which stipulates that the concept should be limited to:[46]

[The protection of] a country's existence or its territorial integrity against the use or threat of force, or [of] its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.

In other countries, the concept of national security may be more limited – but the generic access laws are still sweeping, because the other aims, rather than being brought within the concept, are added to the purposes for which the powers can be used. This is the case in particular in special "anti-terrorist" laws that tend to include many such broader activities within their scope, and grant generic access to communications data (as well as many other "special" powers) to law enforcement and security agencies in relation to such broadly defined matters.

For example, **Myanmar** law allows generic interception not only when the security of the State or the rule of law is adversely affected, but also when it is simply "in the public interest". In **Pakistan**, too, powers of generic access under the Telecom Re-organisation Act (PTRA) can be used in relation to broadly defined purposes and offences. And the recent, special **French** Law on Surveillance over International Communications similarly allows for generic access to ("international", i.e., "external") communications data for the purposes not just of defending the nation or the prevention of terrorism but also, inter alia, in support of "major foreign policy interests" of the state and "major economic, industrial, and scientific interests" of the state, etc. In **South Africa** and **Turkey,** as well, wide powers of generic access are granted in relation to matters well beyond what is covered by "national security" in terms of the Johannesburg Principles.

Understandably, the European Parliament has taken the view that:[47]

a common definition of 'national security' is needed for the EU and its Member States to ensure legal certainty;...the lack of a clear definition allows for arbitrariness and abuses of fundamental rights and the rule of law by executives and intelligence communities in the EU.

"Internal" and "External" (or "International") Communications

In most of the countries surveyed, the relevant authorities are given wide powers to authorise generic access to communications data in relation to the above kinds of widely defined purposes, irrespective of whether the access is to internal (i.e., national domestic) communications or to external ("international") communications. However, in other countries this is seen as an important distinction, for constitutional and historical reasons.

The constitutional justification for the distinction lies in the idea that fundamental rights are "citizens' rights" – i.e., that the rights laid down in a country's domestic constitution are granted to the citizens of the state concerned. It is reflected in the name of the "grandmother" document of human rights, the 1789 **French** *Declaration of the Rights of Man and of the*

Citizen, although in line with modern thinking, in **France** today the main rights set out in the Declaration are now extended to "everyone".

The country in relation to which this is most pertinent in the present context is the **USA**: under **US** law, many of the core constitutional rights – including the First and Fourth Amendment rights – are not extended to non-US persons. However, in the rest of the world this is nowadays an exception, even an oddity. Rather, since the end of World War II and the adoption of the UN *Universal Declaration of Human Rights* in 1946, the basic human rights enshrined in it must be granted by each state to "everyone" within the state's "jurisdiction"—which must be read as meaning, to everyone whose rights are affected by the actions (or inactions) of the state concerned (rather than as having a purely geographical meaning).[48]

There is also a further historical explanation, which is that traditionally the activities of the secret intelligence agencies related to times of war; and in war, it is as legitimate to spy on the enemy as it is to shoot at him.

This historical context helps to explain why in a number of countries other than the **USA** (including the traditionally standard-setting ones) there are laws that allow for the interception of "external" or "international" communications, and indeed for generic access to such communications, on a much less strict basis than applies to access to domestic or internal communications.

For instance, **France**, on 1 October 2015, adopted a new Law on International Communication Surveillance Measures that allows for generic access to "international communications" (metadata and content) on the basis of an authorisation issued by the Prime Minister. In the **UK**, generic access can equally be authorised to such "external"/"international" communications, where it would not be legal to authorise such access in relation to "internal" (UK-domestic) communications. And in **Germany**, too, the Intelligence Services make such a distinction, with little basis for it in domestic law. Most constitutional law scholars agree that the constitution grants the basic right to privacy of telecommunications to anyone. However, in apparent contradiction to this, the treaties **Germany** concluded with the former occupying powers—both before and upon regaining full sovereignty after re-unification—do still often appear to retain such distinctions.[49]

In fact, the "internal"/"external" distinction makes little sense in the era of globalised communications, in particular over the Internet. Thus, Internet communications (e.g., texts or "chats" or VoIP calls, etc.) between two people in one country are still likely to travel through the global Internet infrastructure, including terrestrial and undersea high-speed cables. In the wider global digital communications environment, effectively all communications are "international". States that pretend to limit their surveillance operations by restricting their agencies to the monitoring of "international" communications are therefore essentially disingenuous: in practice, the distinction makes no sense, and many communications that are technically deemed to be "international" are, in fact, between people in their own country.

The "internal"/"external" distinction also loses much of its meaning in the light of the existence of intelligence sharing practices among countries. One participating country's "internal" communications are other countries' "external" communications. When these are shared and combined, their provenance becomes irrelevant. The differential legal treatment of "exter-

nal" and "internal" communications thus serves as little more than a false assurance to one country's citizens and other persons within its territory that their communications enjoy higher protection compared to "foreigners'" communications.

But most importantly, the distinction in protection between "national persons" and "foreigners" – which is effectively what this amounts to – is in fundamental breach of the principle of universality of human rights and of the prohibition of discrimination, inter alia on the basis of nationality or place of residence.[50]

Formal Requirements

Taking the above into account, we may distinguish the following broad schemes of authorisation for generic access to communication data.

In the **USA**, under the Foreign Intelligence Surveillance Act [FISA] and the FISA Amendment Act, the national security agencies (including the NSA) are given effectively unlimited power to intercept in bulk, without a proper targeted judicial warrant, any "foreign" communications, i.e., communications from or to another country, provided that the communications of US nationals and lawful residents ("US persons") are not specifically targeted. This applies to both metadata and content. Similarly, in the **UK**, under the Regulation of Investigatory Powers ACT (RIPA), "external" warrants issued under RIPA s. 8(4)(a) allow for interception of bulk or mass data (metadata or content), whereas "internal" warrants issued under s. 8(1) do not. We now know, thanks to Snowden, that these powers were—and still are—used by the **USA** and **UK** to "hoover up" essentially all data flowing through the undersea cables entering these countries, which carry large proportions of global Internet and other communications data, i.e., for "generic access" to those communications.[51]

But other countries have given similarly sweeping power to their agencies, especially in recent years (even if they perhaps do not have as much access to the Internet and global communications infrastructure).[52] Thus, as noted earlier, **France**, on 1 October 2015, adopted a new Law on International Communication Surveillance Measures that expressly allows the Prime Minister (or someone delegated by him) to authorise, without judicial involvement, the interception of both metadata and contents of "international communication", defined as "communications that are sent to or received from abroad", in relation to counter-terrorism and other serious crime.

In **Germany**, the well-known "Article 10 Law" allows lawful interception and broader communication surveillance, including the "hoovering up" of data in bulk (as long as this does not amount to more than 20% of the cables' total capacity), by the intelligence services in so-called "strategic interception" of similarly defined "international communications"—albeit subject to some restrictions not found in other national laws, in particular that the "strategic interception" must be aimed at terrorism and other serious crimes, and that "key words" used in the filtering of the bulk data must be approved by a special "G10" Commission. However, in the parliamentary committee of inquiry into the Snowden revelations, it was revealed that the main national security agency, the BND, had given excessively broad, "creative" interpretations to the rules, in effect allowing unrestricted generic access. For example, the "20% rule" may have amounted to an effective wiretapping restriction for analogue cable-based telephone communications. But Internet cables only rarely carry more traffic than what amounts to 20% of their capacity, so "hoovering up" up

to 20% of their capacity effectively results in a "full take" of any given cable's traffic. In the inquiry, the former BND in-house lawyer also argued (contrary to the consensus amongst experts in German constitutional law) that foreigners were not subject to the constitutional protection of their communications.[53]
In **Colombia**, the military, the police and the intelligence services may, under Article 17 of Law 1621 of 2013, intercept private telecommunications for the purposes of national security, even where they are not investigating a specific crime. This is, unusually in this context, subject to a judicial order. However, it seems that this safeguard can be evaded by technical means. In the **DR Congo**, in relation to "national security, protection of the essential elements of the scientific, economic and cultural potential of the country, or the prevention of crime and organised crime", the police and the intelligence agencies can be authorised to carry out interceptions of both metadata and content by the Minister of the Interior, without judicial involvement. And in **Egypt**, the 2003 Communications Law gives broad and ill-defined powers to the armed forces and the security agencies (including both the police and the intelligence services) to obtain information (which must be assumed to include communications data, both metadata and content) in relation to "national security" concerns—without defining "national security"; and thus effectively leaving this to the discretion of the authorities.

In **India**, as further outlined in section 4.6, below, there are already broad powers of interception for "ordinary" criminal cases under the CPC; and the Information Technology Act and the Indian Telegraph Act grant even wider powers to a wide range of authorised government officials to intercept or monitor information transmitted, generated, received, or stored in any computer. Furthermore, there are exceptional emergency powers set out in these acts and in the Indian Telegraph Rules that can be invoked, not just when there is an actual emergency, but also "in the interests of friendly relations with foreign states" and "to prevent incitement to commit [any] offences". These provisions grant sweeping powers to order interception relating to whole classes of messages; whole classes of persons; and (it would seem, any) [specified] subject. In effect, these rules also allow for arbitrary, "generic" interception of communications. Similarly, in **Pakistan**, s. 54 of the PTRA allows the Government to authorise "any person" to intercept or trace communications (through the PT Authority), not just in cases of actual emergency, but more broadly in relation to "national security".

In **Kenya**, the National Intelligence Services Act allows interception and monitoring to protect "national security"—but "national security" is defined in Article 238 (1) of the Constitution as including [any] "national interest". Furthermore, the law does not require any kind of targeting of the interception. Given this sweeping definition of "national security" and absence of substantive limitations, the procedural safeguard of a High Court judge's warrant cannot be regarded as effective. In **Myanmar**, s. 77 of the Telecommunications Law 2013 gives the government broad powers of interception on a number of vaguely stated grounds, including when it is in the "public interest", and when the security of the State or the rule of law is adversely affected.

In **Russia**, no court order is required for access to metadata, neither by the police nor by the intelligence services. Such an order is required for access to content data, but in cases relating to national security no suspicion or

evidence of any specific criminal offence needs to be shown. Thus, if the authorities claim a national security issue is at stake, the court is given little leeway to deny the order (even if it were to be so inclined). Under the country's Counter-Terrorism Law, moreover, the national security agency, the FSB, can also more broadly take control of private communications, also outside of a declared emergency. Presumably, this includes the power to demand unrestricted access to communications data, both metadata and content. Whether this power is used in this way, we do not know.

And finally, in **Turkey**, interception of communications (both metadata and contents) can be ordered on grounds of "national security, public order, prevention of crime, protection of public health and public morals, protection of the rights and freedoms of others". In "normal" cases, this requires a court order but in "non-delayable" cases, it suffices if a written order has been issued by any "agency authorised by law", which includes the security services. The law does not define what "non-delayable" cases are. Moreover, the Information and Communication Technology Authority, BTK, can also order the interception of communication data (again, both metadata and contents) for the purposes of protecting public safety and "public interests", after obtaining a (positive) "opinion" on this from the Ministry of Transport and Communications.

Technical requirements (including a requirement to install a "back door"); and the "hacking" of systems without the knowledge or cooperation of providers

Legally imposed "back doors" [54]

It is clear from the operators' information provided through the TID website that most, indeed probably all, countries impose "technical requirements" on TSPs and (M)NOs, which require them to install equipment to "facilitate" both specific "lawful intercepts" and the "generic access" discussed in this section.

Vodafone is, as far as we can see, the only provider that has further commented on this, pointing out that:[55]

the lawful interception technical standards set down by the European Telecommunications Standards Institute (ETSI), which define the separation required between the agency or authority monitoring centre and the operator's network [and which] are globally applicable across fixed-line, mobile, broadcast and internet technologies [stipulate that there should be] a formal handover interface to ensure that agencies and authorities do not have direct or uncontrolled access to the operators' networks as a whole.

The inclusion of a "handover interface" is of course crucial, because if the TSPs and (M)NOs cannot see what access the authorities in practice have to their systems, this seriously undermines any oversight and accountability systems. As the European Court of Human Rights put it in its recent *Zakharov* judgment:[56]

a system...which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. [Moreover, a] prohibition on logging or recording [of] interceptions... makes it impossible for the supervising authority to discover interceptions carried out without proper judicial authorisation. Combined with the law-enforcement authorities' technical ability...to intercept directly

all communications, [such a prohibition] renders any supervision arrangements incapable of detecting unlawful interceptions and therefore ineffective.

However, as far back as 2001, the ETSI standards were severely criticised for effectively allowing indiscriminate ("comprehensive") surveillance by law enforcement and national security agencies, because although the protocol stipulates that only the service providers should use the specified (numerous) search commands, there is no check on this.

In any case, Vodafone adds that in practice:
In most countries, Vodafone maintains full operational control over the technical infrastructure used to enable lawful interception upon receipt of an agency or authority demand. However, 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.

Thus, although Vodafone "continuously encourage[s] agencies and authorities to conform to ETSI technical standards", in some countries those standards are clearly not complied with, and direct-access "back doors" are installed that allow unmonitored—and unmonitorable—access to the provider's systems by the security agencies.

We also have doubts as to the supposedly "full operational control" that is said to be retained by Vodafone (or any TSP). As Vodafone explains:
In each of our operating companies around the world, a small number of employees are tasked with liaising with agencies and authorities in order to process demands received. Those employees are usually security-cleared to a high level and are bound by law to absolute secrecy. They are not permitted to discuss any aspect of a demand received with their line management or any other colleagues, nor can they reveal that a demand has been received at all, as doing so could potentially compromise an active criminal investigation or undermine measures to protect national security. Additionally, in some countries, they cannot even reveal [NB: even to their own line managers or employer] that specific law enforcement assistance technical capabilities have been established within their companies.

Vodafone claims that it "can – and do[es] – challenge demands that are not compliant with legal due process or seem disproportionate". However, given that (as it acknowledges in the same sentence) it cannot know the purpose of an access request, it is difficult to see how it can assess its proportionality. Presumably, all this means is that if any of the specially vetted and selected employees were to note a clear breach of relevant formal requirements (e.g., the absence of a required [electronic] signature on a request form), she or he could report this to her or his line manager, and Vodafone could refuse to comply with the order. But we cannot see how any telecommunications service provider could effectively challenge access demands on grounds other than such obvious formal non-compliance. The employees in question, moreover, who are all extensively vetted

by the security agencies and often had earlier links with them, are likely to be torn in their loyalties between the security agencies and their formal employer, the TSP.

From the information available on the 14 countries included in our survey, it is not always clear whether the "technical requirements" in a country can include a requirement to build in a "back door" into the TSPs' and (M)NOs' systems, and if so whether the "back door" can be used by the authorities to gain direct access to all the data in these systems, or to all the metadata or all the contents data without the TSPs and (M)NOs being able to see what exact use is made of the "back doors". However, from our sample, it would appear that the imposition of "back doors" is more widespread than the Vodafone Law Enforcement Disclosure Report 2014 suggests.[57]

We know that, under its PRISM programme, the **US** NSA has demanded direct (generic) access to the systems of **US** TSPs and (M)NOs and globally operating **US** Internet Service Providers and social networks, including Google, Facebook and Apple[58] —with the companies in question being placed under a "gagging order", legally preventing them from informing their customers (the data subjects) anywhere in the world, or even the data protection authorities in the relevant countries, including the EU Member States, of the fact that their data are thus directly and indiscriminately accessible to and accessed by the **US** NSA.

In the **UK**, a 2002 Order issued under the Regulation of Investigatory Powers Act (RIPA), and indeed RIPA Part III and the Intelligence Services Act, can all be read as allowing the imposition of "back doors", but it is unknown whether this is done under these instruments. However, the broadest of all provisions is s. 94 of the Telecommunications Act 1984. This gives the government the power to issue "directions" to providers of public electronic communications networks to do, or not to do, anything. It was long suspected that this power was used in relation to the surveillance programmes revealed by Edward Snowden, but this has only recently been confirmed formally by the government, after it had been urged to "avow" (i.e., own up to) the use of the power to gain direct, bulk access to communications (i.e., metadata), by the official reviewer of the legislation, David Anderson QC.[59] Anderson revealed that both he and Parliament's Intelligence and Security Committee (the official oversight body over the intelligence services) had been told of this use of the power, but had been barred from revealing it in their reports. Given the utterly unfettered power to order anything, s. 94 can clearly also be used to order even wider "back doors", providing direct access to content of communications, even if this has not been "avowed". It is, in any case, difficult to see how the reported restriction of the now-revealed "back doors" into metadata can be limited to such data – or who can really oversee this. In the light of the Snowden revelations, we feel it would be surprising if in this regard the **UK**'s GCHQ was not using such devices in ways similar to the **US**'s NSA.

But it would appear that these practices are far from limited to the **UK** and the **USA**.

In **Colombia**, too, TSPs and (M)NOs may be required to install technical equipment to facilitate interception and monitoring (under Decree 1704 of 2012); and certain officials, rather confusingly referred to as "judicial

police"[60] may access the TSPs' and (M)NOs' networks via officially mandated "connection and access points" for the purpose of giving effect to a judicial intercept order (Constitutional Court Decision C-594). It seems likely that these "connection and access points" amount to a "back door". In **Kenya** and **Pakistan**, the law also requires the installation of devices allowing direct access. In the **DR Congo**, the law is so sweeping that it must be assumed the authorities can also demand this. In **South Africa**, the law is complex but is said to not allow for mandatory installation of "back doors".

In **Russia**, the "Rules on Cooperation" that set out the terms of the relationship between the TSPs and (M)NOs and the Intelligence Services require the installation of "back doors". Similarly, in **Egypt**, the military authorities can demand access to the TSPs' and (M)NOs' infrastructure, without the TSPs or (M)NOs being able to check how this access is used. Moreover, Privacy International reported that the Egyptian government has the technological capacity to carry out surveillance of social media users, to access their accounts and identify potential dissidents, activists, and journalists as well as citizens who are speaking out against the government.[61]

Elsewhere, mandatory access arrangements are imposed under the licenses that TSPs and (M)NOs must obtain in order to provide their services, and with which they must comply on penalty of losing the license. Thus, in **India**, according to the TID information:

Clause 34.8 of the ISP License, requires each ISP to maintain a log of all connected users and the service that they are using. The ISP is also required to maintain every outward login. The logs and the copies of all the packets originating from the Customer Premises Equipment ("CPE") of the ISP must be available in real time to the government.

In 2013, it was reported in the Indian press that a "Centralised Monitoring System" (CMS) would be established by the end of that year, as part of "an ambitious program that will let [the authorities] monitor any one of its 900 million telecom subscribers and 120 million internet users." According to the reports:[62]

with the CMS, security agencies won't need to request users' information from [telecommunications companies]. They'll be able to get it directly, using existing interception systems that are built into telecom and data-service networks. According to the Hindu newspaper, the system will have dedicated servers and extensive data-mining capabilities that can be used for surveillance.

In **Myanmar** too, the relevant licenses may impose effectively any requirement on the service providers, including allowing the installation of "back doors". And in **Turkey**, the ICT Authority, BTK, can impose conditions on TSPs and (M)NOs that include technical requirements for interception which, again, amounts to mandatory "back doors".

In sum: it would appear that in the vast majority of the countries surveyed, there are laws or rules that can be read as allowing the authorities to demand that TSPs install "back doors" into their systems. And in most, if not all of these situations, the TSPs can be prevented from reporting on this. In our view, it is likely that in many of the countries surveyed, such "back doors" are imposed and subject to secrecy, but by definition we cannot provide reliable statistics on such secret practices.

The laws and rules in other countries are less clear. In **France**, the Code on Mail and Electronic Communications requires TSPs and (M)NOs to "implement relevant internal processes" to "respond to requests for access" to data, which suggests that there is some control by the TSPs and (M)NOs over the responses to those "requests" from the authorities. And in **Germany**, the TSPs and (M)NOs must also "assist" in the implementation of interception. The detailed requirements and specifications, including required technical and organizational standards are contained in published regulations, the Telecommunications Interception Ordinance, and the Technical Directive issued under it. We cannot judge whether the technical specifications in these rules suffer from the same alleged defect as the "mother" ETSI standards that inspired them. If so, this would in practice lead to direct access without the knowledge or involvement of the TSPs and (M)NOs. In any case, in these last two countries surveillance programmes have been exposed that suggest the Intelligence Services in any case do tap directly into the main Internet and electronic communication cables running to or from or through their territories (including, in the case of **France**, its overseas territories).

The "hacking" of systems

In a way, the question of whether the above laws can be read as requiring TSPs and (M)NOs to install "back doors", and/or whether the installation of such devices have in fact been imposed on them, has become somewhat moot when it comes to the countries most deeply involved in the global surveillance programmes exposed by Edward Snowden, the **USA**, and the **UK**. As Snowden revealed in 2013, the **UK**'s GCHQ and the **US**'s NSA have developed "hacking" techniques to create "back doors" without any involvement of the "hacked" companies. These highly advanced technologies have also been used to try and access encrypted data streams of Internet communication services, including Hotmail, Google, Yahoo, and Facebook.[63] Whether other technologically advanced states, such as **Russia** and **China**, have developed similar technologies is unknown, but it would be surprising if they have not at least been trying to acquire them, and there are some reports that may suggest this.[64]

Such "hacked" access is, by its very nature, almost impossible for TSPs and (M)NOs and others to detect, and thus to report on. Moreover, any revelation of such security breaches (if discovered *ex post facto*) would undermine the trust that their customers have in them, which is a serious disincentive to disclosure. However, in the future, under the new EU General Data Protection Regulation (due to be adopted by the end of 2015 and to come into force in 2017), companies operating in the EU would be required to report such data breaches.

Oversight

The TID information shows that in six of the countries studied **(DR Congo, Egypt, Myanmar, Pakistan, Russia** and **Turkey)**, there is effectively no independent oversight over the use of the above-mentioned powers of "generic access", not even on paper. At most, in some of these countries (like **Myanmar** and **Russia**), there are internal oversight systems by officials or bodies that are part of the executive branch, but these are by their very nature not independent or detached from the system.

In **France**, the use of the generic access powers provided for in the recent law is only subject to "advice" from various bodies, rather than real over-

sight. In **India**, there is oversight only by a "review committee" made up of high officials, but by law the committee must maintain "utmost secrecy" and destroy its own files after six months.

In other countries studied, oversight systems are in place but they have proved to be ineffective. This is, in particular, the case in the two countries to which the Snowden revelations related most directly: the **USA** and the **UK**. As detailed analyses by international and national NGOs have shown, because of inherent defects, in neither country did the systems serve to stem or temper indiscriminate surveillance and "generic access" in relation to "external" communications.[65] In the **UK**, various oversight commissioners are not independent and report to the Prime Minister. The members of the parliamentary oversight committee, the ISC, are also appointed by the Prime Minister, and its reports are moreover subject to redactions and deletions by the Prime Minister. The Investigatory Powers Tribunal has limited powers and its processes are nontransparent. None of the above even flagged the mass surveillance programmes until Snowden revealed them; none sought to restrain them.

The situation in the **USA** is no better. The Foreign Intelligence Surveillance Court, or FISC, has no jurisdiction over many of the most important surveillance activities, including those authorised under Executive Order 12333. As the leading US NGOs that analysed the system put it:[66] "What little oversight the FISC exercises is severely hampered by a near total lack of transparency about its proceedings and decisions." Moreover, it effectively has to rely on the intelligence agencies themselves to report and correct non-compliance with the law. FISC itself found that the privacy safeguards it imposed on the government's telephone metadata programme:[67]
[had] been so frequently and systematically violated that it can fairly be said that this critical element of the overall regime has never functioned effectively.

Moreover, if remedies for US nationals and foreigners living in the USA ("US persons") are weak and ineffective, for "non-US persons" they are "even more illusory".[68]

Indeed, the absence of any real remedies for "non-US persons" in the **US** system led to major tensions between the **USA** and the EU. An "Umbrella Agreement" for data protection in relation to law enforcement data exchanges between the EU and the **USA** (initialled but not yet signed by the parties), which was hailed as leading to judicial redress for EU persons in the **USA**, in fact falls far short of international and EU-constitutional minimum requirements. It also falls short in terms of remedies, especially for non-EU citizens whose data might be transferred from the EU to the USA under the agreement.[69] Specifically, the Umbrella Agreement would not prevent data transferred by EU-based law enforcement agencies to US law enforcement agencies from being shared with to the US national security agencies. There are no remedies against this data sharing if that is allowed under the law of the USA, as it quite generally is.[70]

Even in countries that appear on paper to have halfway decent systems of oversight, these are still often undermined or bypassed. For instance, although in **Colombia** the law requires a judicial order for interception of contents of communications, oversight over whether such an order is always obtained, and if it is valid (e.g., if it is sufficiently precise) is under-

mined not only by the well-known general deficiencies in the judicial system, but also, by the fact that the authorities can apparently demand the installation of "back doors" into the TSPs' and (M)NOs' systems: the use of such "back doors" is by their nature often impossible to monitor. Suspicions in this regard are heightened by reports of apparently widespread surveillance outside of the law. Similarly, in **Kenya**, the law requires judicial authorisations for interception and there is a parliamentary committee that nominally has powers of oversight over surveillance. However, the legal system is weak and it is suspected that these safeguards are widely circumvented. In **South Africa**, too, the requirement of judicial authorisation is undermined by the fact that it can be given by special, government-selected, "designated" (e.g., retired) judges,[71] and by the low threshold required for authorisations. There have also been reports of serious abuses, which were not prevented by these requirements.[72]

In **Germany** there is, in principle, some serious oversight by the "G10 Commission", that involves members of Parliament and has a direct say in the choice of "key words" or "selectors" used in the filtering of data obtained through "strategic interception". However, this oversight has not prevented secret and apparently indiscriminate interception from taking place, on the basis of "creative" interpretations of the law by the intelligence agencies, of which the G10 Commission was apparently unaware.[73]

Transparency

In this sub-section, we discuss two aspects of transparency: first, transparency about the rules that govern surveillance, in particular "generic access"; and second, transparency about the use of those powers in practice.

Transparency about the law

The rule of law implicitly requires that all legal rules—and certainly all legal rules that in any way interfere with or limit fundamental rights—should be publicly accessible. This requirement flows from the very concept of "law" as interpreted by the international and regional human rights courts and fora. This also applies to interpretations of those rules, since they clarify what they mean and how they will be applied. If they are interpreted in secret and in ways that are not obvious from the text itself, the law lacks the required "foreseeability".[74]

Although one would therefore assume that in all countries the laws and rules relating to surveillance would be publicly accessible, this does not appear to be as widespread in reality. The TID information on which we draw for our analysis has specific information on legal rules relating to surveillance apparently being allowed to be kept secret in three countries. In **Colombia**, all laws must be published, but the report adds that this is the case "unless another law states otherwise". There is no information as to whether this exception actually applies in relation to surveillance, and if so, what those "other laws" might be. In relation to **Pakistan**, the TID information refers to the Freedom of Information Ordinance, from which it follows that in principle all legal rules should be accessible (because they constitute information in the hands of public authorities). However, this makes such access subject to the broad exceptions to access, contained in the Ordinance, in particular in relation to widely defined matters of "national security". This suggests that certain rules relating to surveillance, in particular subsidiary rules or internal guidance and interpretations of those

rules, can be kept secret. In **Russia**, the laws on communications and information prohibit TSPs and (M)NOs from revealing information about any tactical or organisational actions taken or methods used by the country's secret intelligence agencies to conduct investigations by using data from a network operator's network, and it is suggested that this prohibition could be construed so widely as to prevent the agencies from even publishing the laws and regulations to which they are subject, even though these laws are not legally regarded as confidential and even though there is no specific regulation to prohibit the operators from publishing information relating to these laws. It seems to be implied that although on the face of it there is nothing in law to prevent operators from publishing the rules under which they are required to operate, in practice they feel they might be vulnerable if they did publish them.

The TID information does not provide any information as to whether the laws and interpretations are publicly accessible in relation to no fewer than 10 out of the 14 countries concerned:[75] **DR Congo, Egypt, France, Germany, India, Kenya, Myanmar, South Africa, Turkey** and the **UK**. In some of those countries there are serious concerns about adherence to the rule of law in general. In such cases, it may be assumed that, although perhaps not whole primary laws, then at least subsidiary rules and instruments and internal guidance on and interpretations of the primary rules are kept secret, and/or subject to arbitrary application. Based on our research and interviews, this is likely to be the case in **DR Congo, Egypt, Kenya** and **Myanmar**; and it also quite probably the case that there are such secret rules or guidelines or interpretations in India, South Africa and Turkey. In Zakharov, the European Court of Human Rights found it "regrettable" that there was a "lack of a generally accessible official publication" of the detailed rules on interception in **Russia** (although it did not find a violation of the ECHR in this regard since the applicant had been able to unearth the rules from an Internet legal database).[76]

Furthermore, even in the countries that publicly hold themselves out as models for the rule of law, such as the **USA**, there have been worrying departures from the principle that all legal rules and interpretations should be publicly accessible and foreseeable. Since the revelations about the secret "torture memos" on which the **USA** relied to systematically violate the *ius cogens* norm (peremptory principle of international law) prohibiting such treatment,[77] we have learned that even in that country, which prides itself on the strength of its Constitution, those principles are ignored at times. And we now know that this has also happened in relation to the NSA's mass surveillance programmes.[78] The most notorious example of this is the expansive, secret interpretations of the terms "relevant", "business records" and "tangible things" in the infamous section 215 of the USA PATRIOT Act, which allow the NSA to collect massive amounts of communications data on "US persons", contrary to what most experts on US constitutional law (and even the original sponsors of the PATRIOT act) had assumed to be lawful until the secret rulings were revealed after litigation.[79]

Similarly, in the **UK**, the detailed rules governing the country's surveillance activities under broadly phrased statutory provisions (and those governing its data sharing arrangements, in particular with the **USA**) were kept completely secret until February 2015, when the Investigatory Powers Tribunal ruled that this was contrary to the Human Rights Act, following which

some small, selective portions of the policies were made public. However, most of the detailed rules issued under, and interpretations of, the law remain secret. This secrecy is currently being challenged by Privacy International and nine other human rights organisations in the European Court of Human Rights.[80]

The recent **French** surveillance law, adopted on 1 October 2015, contains a provision which allows for secret decrees by the *Conseil d'État* to regulate the detail of the relevant surveillance (Article L. 854-1).[81] This has been criticised by human rights groups, lawyers and magistrates, who pointed out that, for instance, the term "international communications" could be subject to such secret interpretations, and thus stretched in the same ways that **UK** law had secretly been stretched.[82]

As already noted, in **Germany**, too, the former in-house lawyer for the main intelligence service, the BND, has revealed that the agency relied on "creative" interpretations of the law to carry out surveillance operations, including tapping into the global communication systems, in ways that lawyers had until then be assumed to be unlawful. Indeed, contrary to a consensus amongst constitutional lawyers, he argued that the constitutional protection of confidentiality of communications did not apply to foreign people outside Germany – and the BND appears to have been acting on that basis.

The Parliamentary Assembly of the Council of Europe was clearly addressing its own member states when it unambiguously condemned, in no uncertain terms:[83]

the extensive use of secret laws and regulations, applied by secret courts using secret interpretations of the applicable rules, as this practice undermines public confidence in the judicial oversight mechanisms.

Transparency About Practice

In four countries, **Colombia, Pakistan, South Africa** and the **UK**, the law expressly forbids the release, by TSPs and (M)NOs, of information on the use of lawful intercept and broader "generic access" surveillance powers, including aggregate information. With regard to **Colombia**, TID notes that Article 33 of Law 1621-2013 "allows the Intelligence and Counter-Intelligence Services to prevent the publication of aggregate data." It does not say whether the services actually used this power, but it could be assumed from the absence of such aggregate data in the TID information that the powers have been so used. In **Pakistan**, the situation is if anything even more straightforward: disclosure of all information about interceptions, including the publishing of aggregate data, is simply forbidden (although of course occasionally some information may come out in court). Privacy International also confirms that telecommunications companies in Pakistan are barred from publishing information, including aggregated statistics, regarding interception of both communications contents and metadata.[84]

In **Russia**, as further discussed in section 4.10, Article 64 of the Law on Communications and Article 10.1 of the Law on Information stipulate that Network Operators and so-called "Pure" Internet Service Providers may not disclose any information about any tactical or organisational actions taken, or methods used by, the intelligence services, including both targeted lawful intercepts and "generic access". It may be because of this that the operators involved in TID have not released statistics on **Russia**. However,

the Constitutional Court apparently does release statistics on the number of warrants issued. These are quoted in the *Zakharov* judgment of the European Court of Human Rights as follows:

The applicant also produced official statistics by the Supreme Court for the period from 2009 to 2013. It could be seen from those statistics that in 2009 Russian courts granted 130,083 out of 132,821 requests under the CCrP [Code of Criminal Procedure] and 245,645 out of 246,228 requests under the OSAA [the Operational-Search Activities Act] (99%). In 2010 the courts allowed 136,953 out of 140,372 interception requests under the CCrP and 276,682 out of 284,137 requests under the OSAA. In 2011 the courts allowed 140,047 out of 144,762 interception requests under the CCrP and 326,105 out of 329,415 requests under the OSAA. In 2012 they granted 156,751 out of 163,469 interception requests under the CCrP (95%) and 372,744 out of 376,368 requests under the OSAA (99%). In 2013 the courts allowed 178,149 out of 189,741 interception requests lodged under the CCrP (93%) and 416,045 out of 420,242 interception requests lodged under the OSAA (99%). The applicant drew the Court's attention to the fact that the number of interception authorisations had almost doubled between 2009 and 2013.85

As already noted, however, the Court also held that, since the law expressly prohibited the keeping of logs or records on "direct access" to communications (content and metadata) by means of "back doors", it was impossible to verify whether such access had occurred without warrants.

In the **UK**, release of such information is prohibited under s. 19 of the Regulation of Investigatory Powers Act.

The TID information does not include information on the situation in this regard in the other nine out of the 14 countries included in the survey:[86] **DR Congo, Egypt, France, Germany, India, Kenya, Myanmar, Turkey** and the **UK.** We may again assume that in **DR Congo, Egypt** and **Kenya** this is likely to be the result of this having been made clear to the TSPs involved in TID. This may also be the case in **India** and **Turkey**.

With regard to **Myanmar**, there is the rather odd datum in a Telenor report with country information that during October-December 2014 there had been nine instances of some relevant use of interception powers, but this is referred to as "historical data", which may mean data on the history of uses of telecommunication systems of devices, i.e., certain metadata (the corresponding entries in the other country sections is headed "communication data", not "historical data"; there is no explanation of this).[87] There is no entry under the heading "Lawful interception". Although a related Telenor report on the legal issues says that "There is no law in Myanmar preventing the publication of aggregate data relating to the use of the powers described above",[88] it would therefore appear that in practice, either the TSPs and (M)NOs do not know what use is made of the relevant powers, or that the company is effectively prevented from publishing the relevant data, even though there is no law prohibiting it.

With regard to **France, Germany** and the **UK**, the authorities themselves do provide some (albeit rather limited, censored, and disputed) information on the use of their surveillance powers. Regrettably, the operators involved in TID do not provide their own statistics on these countries, or comment on the ones released by the authorities.[89]

Thus, in the **UK**, information is made available by the authorities on the number of warrants used for targeted interception warrants issued under s. 8(1) of RIPA, but it is limited to the issuing of such warrants by bodies other than the intelligence agencies, including law enforcement agencies. According to the most recent report by the Intelligence Services Committee:[90]

The total number of new Section 8(1) warrants issued in 2013 was 2,757. (The number of extant Section 8(1) warrants as at 31 December 2013 was 1,649.) These include all nine bodies authorised to conduct interception under RIPA.

However, the report refrains from revealing more specific statistics and offers an explanation for the retraction in the text:

We have been given the number of 8(1) warrants for MI5, SIS and GCHQ (*, *** and *** respectively). However, we cannot publish these figures since they would provide an indication of the Agencies' investigatory capacity.**

As already noted, the **UK** TSPs and (M)NOs are also barred from revealing these numbers (or rather, the corresponding numbers for each of these providers).

The report is similarly obscure in relation to the use, by the intelligence services of the wider ("generic access") s. 8(4) authorisations – although it does provide this snippet of information:[91]

...during 2013, the [Intelligence] Agencies submitted a total of 58,996 notices or authorisations for CD [Communications Data = metadata] to CSPs [Communications Service Providers] (MI5 submitted 56,918, GCHQ submitted 1,406 and SIS submitted 672).

But the report shows that this probably constitutes only a fraction of the metadata collected by the agencies, because it makes clear that they also extract "communications data" (metadata) from the communications they intercept in bulk (without involving the service providers); and that they can receive such data from their "overseas partners", including the **US**'s NSA. The volumes of metadata thus collected are deleted from the published report.[92]

In **Germany**, the Ministry of Justice annually publishes details of the use of lawful intercept powers in relation to criminal investigations. The "G10 Commission" that supervises the intelligence services publishes details of the use of these powers by the intelligence services. The most recent G10 Commission Report, from March 2013, indicates that the number of authorisations issued to the intelligence services for targeted interception is less than 100 in each half year, and affected between 800 and 900 individuals in each period (including both primary and secondary targets).[93] According to the same report, in relation to "international terrorism", in the first half year of 2011, the G10 Commission authorised the use of 1450 "key search words" for the filtering of generically accessed information (i.e., of information accessed under what the Germans call "strategic surveillance" or more precisely "strategic limitations" on [read: interferences with] the right to confidentiality of communications, Strategische Beschränkungen nach § 5 G 10); and 1660 such key words in the second half of that year. In 2011, 329,628 communications were further examined in this context. Of these communications, 327,557 were emails. However, in the previous year (2010), some 10,213,329 communications had been further examined, including 10,208,525 emails. The report says that this did not

include any internal communications within Germany, and that the BND claimed this was a spike resulting from "a spam wave". An official review of BND practices resulted in the large reduction in numbers. Of the 329,628 communications that were further examined in 2011, 136 were ultimately marked as "relevant for intelligence purposes"; in 2010, it had been 29.[94]

The comparative numbers of "key terms" in relation to weapons proliferation were 13,521 and 13,786 for 2011 and 2010 respectively, leading to further examination of 2,544,936 communications in 2011, compared to 27,079,533 in 2010. Of these, 56 were marked as relevant for intelligence purposes in 2011; the figure for 2010 had been 180.[95] In relation to international trafficking (presumably, of human beings), 348 key words were authorised in the first half of 2011, and 294 in the second half, leading to further examination of 436 communications. In 2010, 45,655 communications had been further examined. In 2011, 98 communications were marked as relevant for intelligence purposes in this context.

However, media have reported that in fact the BND alone collects some 220 million telecommunication datasets *each day,* and retains about 1% indefinitely[96] which suggests that its data mountain is growing daily by more than 2 million datasets.

The report also says that although the G10 Law allows the **German** intelligence services to disclose personal data obtained as a result of "strategic surveillance" to "specific foreign public bodies", this did not happen in 2011 or 2010.[97] This claim also appears to be untrue.

Given that the **French** law on surveillance over international communications has only just come into force, statistics are not yet available on its use. However, as with **Germany**, there have been revelations about extensive surveillance even before the law was adopted, clearly outside the law.

Finally, regarding the **USA** (which is not covered by the TID information), the first and main point that should be made is that such official information as is available has come from the Snowden revelations; the **US** Government is extremely reticent about what it is really doing, and about the actual programmes and statistics. The Fourth Periodic Report of the United States of America to the United Nations Committee on Human Rights Concerning the International Covenant on Civil and Political Rights, for review in the UNHRC's Universal Periodic Review of the **USA** in 2011, did not include any details of the actual programmes later revealed by Snowden, and contained no related statistics.[98]

A classified document produced in secret litigation before the Foreign Intelligence Surveillance Court, originally marked "TOP SECRET/NCS/SI/NOFORN" ("NOFORN" indicating "no foreigners") but later obtained by the ACLU in separate litigation, expressly confirmed that in **US** legal thinking, "there is no constitutionally protected interest in metadata, such as numbers dialled on a telephone".[99] It also confirmed, indirectly, that the **US**'s NSA copies and stores effectively all the metadata on all the communications to which it has access:[100]

Collecting and archiving metadata is thus the best avenue for solving the following fundamental problem: although investigators do not know exactly where the terrorists' communications are hiding in the billions of telephone calls flowing through the United States today, we do know that they are there, and if we archive the data

now, we will be able to use it in a targeted way to find the terrorists tomorrow...As the NSA has explained, "[t]he ability to accumulate a metadata archive and set it aside for carefully controlled searches and analysis will substantially increase NSA's ability to detect and identify members of al Qaeda and its affiliates."

The "carefully controlled searches and analysis" referred to are clearly searches and analyses of the "archived"/"set aside" full copies of the metadata relating to "billions" of communications.

Neither the Patriot Act, nor FISA, nor the FISA Amendment Act places any meaningful restrictions on the collection and "archiving" or "setting aside" of information on the communications involving "non-US persons". In other words, the contents of communications of "non-US persons" may be as indiscriminately collected as metadata on the communications of "US persons" and "non-US persons".[101] The inference is that the NSA collects as many of these "non-US" communications as it can and stores them, within technical limitations only, for later searching and analysis.

This is confirmed by the information "leaked" by Snowden which shows, inter alia, that under its UPSTREAM programme, the NSA copies communications and data passing through networks that connect North America to the rest of the world; that pursuant to Executive Order (EO) 12333, the **US** government collects and stores for thirty days a recording of every single call made in or out of at least two entire countries, including the Bahamas; and that the government intends to expand the program, called MYSTIC, to more countries (if, as **US** NGOs noted, if it has not already done so).[102] To again quote the NGOs:[103]

The NSA also sweeps up communications data (e.g., e-mail address books and contact lists) outside the United States through methods such as tapping into fiber optic cables that connect the data centers of major Internet companies around the world. For example, under a program code-named MUSCULAR, the NSA and the UK intelligence agency GCHQ reportedly tap into internal Yahoo and Google networks to collect data from hundreds of millions of user accounts. This data is temporarily held in a digital "buffer," and sent through a series of filters to "select" information the NSA wants. Between December 2012 and January 2013, the NSA "selected" and sent back to its headquarters 181,280,466 new records of communications data. Programs like MUSCULAR also operate pursuant to EO 12333, which authorizes the interception of signals to collect information for a broad range of "foreign intelligence purposes." There is little doubt that such activities impact the communications and privacy of a large proportion of the world's population. Recent statements from a former U.S. official confirm this.

In conclusion, there is little official transparency on the part of **USA** officials regarding either the details of the NSA surveillance programmes, or on the numbers of global communications that are affected by them. It is implicit in the statements by the authorities, however, that there are essentially no legal limitations on those numbers. Moreover, as a result of the Snowden revelations and of litigation by US NGOs, it has been confirmed that the data amounts to literally *trillions* of datasets of *billions* of individual communications, collected and at least temporarily archived in massive NSA databases.[104]

Three Caveats

To the above comparative overview, we must add three caveats. First of all, with reference to the Zakharov judgment, if TSPs and (M)NOs are forced to install back doors into their system through which various agencies can obtain direct access to their systems, and if this direct access is unmonitored – and unmonitorable – by those providers and operators, this of course seriously undermines any oversight and accountability or transparency systems. This applies even more clearly if their systems are "hacked" behind their backs.

Secondly, as Vodafone has pointed out in its transparency reports, it is in practice very difficult, especially for TSPs and (M)NOs, to issue meaningful statistics, for several reasons:[105]

First, no individual operator can provide a full picture of the extent of agency and authority demands across the country as a whole, nor will an operator understand the context of the investigations generating those demands. It is important to capture and disclose demands issued to all operators: however, based on our experience in compiling this report, we believe it is likely that a number of other local operators in some of our countries of operation would be unwilling or unable to commit to the kind of disclosures made by Vodafone in this report.

Second, different operators are likely to have widely differing approaches to recording and reporting the same statistical information. Some operators may report the number of individual demands received, whereas others may report the cumulative number of targeted accounts, communications services, devices or subscribers (or a varying mixture of all four) for their own operations....Similarly, multiple different legal powers may be invoked to gain access to a single customer's communications data: this could legitimately be recorded and disclosed as either multiple separate demands, or one.

To add to the potential for confusion, an agency or authority might issue the same demand to five different operators; each operator would record and disclose the demand it received in its own way (with all of the variations in interpretation explained [later]); and the cumulative number of all operators' disclosures would bear little resemblance to the fact of a single demand from one agency. Moreover, in countries where the law on disclosure is unclear, some operators may choose not to publish certain categories of demand information on the basis of that operator's appetite for legal risk, whereas another operator may take a different approach, leading to two very different data sets in the public domain.

In its 2014 report, Vodafone explained that it:[106]

focused on the number of warrants (or broadly equivalent legal mechanism) issued to our local businesses as we believe this is the most reliable and consistent measure of agency and authority activity currently available. The relatively small number of governments (9 out of the 29 countries covered in this report) that publish aggregate statistics also collate and disclose this information on the basis of warrants issued.

It felt that "disclosure of the number of individual warrants served in a year is currently the least ambiguous and most meaningful statistic when seeking

to ensure public transparency." However, it acknowledged that each warrant could cover interception of metadata or contents relating to the communications of several, sometimes a great many, individuals, and to numerous different devices. In the UK, a single "external warrant" issued under s. 8(4) RIPA could conceivably[107] "specify 'all communications entering and leaving the British Isles', or all such communications carried on a particular cable" and (as the expert Jemima Stratford QC added) such extremely broad single warrants, covering the communications of millions of individuals, may well be precisely what is required in order to carry out keyword analysis.

We agree that governments should also compile and release meaningful statistics on the use of their interception powers. We feel that such statistics should also cover:

- the number of warrants or authorisations issued;
- the number of communication outlets or cables affected; and
- the number of individuals affected by them.

Our third and final caveat to the discussion on transparency in this subsection is that, if the intelligence agencies operate programmes outside the law—as many do—then those "extralegal" programmes are of course also outside of any formal oversight or transparency framework. They are thus, by their very nature, completely nontransparent.

2.3.5 Special Powers in Official Emergencies

The focus of this report is on the use of broad surveillance powers for anti-terrorism and "national security" purposes outside times of war or officially declared national emergency (an "emergency threatening the life of the nation", as it is put in the international human rights treaties). However, we may note briefly that in many countries the executive powers can assert special powers, and largely suspend many fundamental rights, in times of war or formal emergency.[108] It is clear from the TID information that in many of the countries surveyed, in such exceptional times the authorities have extremely broad special powers to impose duties or restrictions on TSPs and (M)NOs, or indeed to take over their operations.[109]

These powers are essentially discretionary in **DR Congo, Egypt, Kenya, Myanmar, Pakistan, Russia, South Africa, Turkey** (especially if martial law is declared) and the **UK.** In **France** (and in other countries that derive their legal system from the French model), extremely broad powers accrue to the executive branch or the military in formal states of war and siege *(états de guerre et de siège).*[110]

In **Germany**, the Constitution as adopted in 1949 (the Basic Law or *Grundgesetz*) originally did not refer expressly to states of emergency. Prior to the country regaining full sovereignty after its reunification, the occupying powers reserved for themselves the right to intervene in such cases. But in 1968, against much popular protest, the **German** legislator adopted the so-called "Emergency Laws" (*Notstandsgesetze*) under which some otherwise constitutionally guaranteed rights, including the right to confidentiality of communications, could be temporarily suspended. In **India**, too, many fundamental rights, including the right to confidentiality of communications, can be suspended in times of "national emergency".

In contrast, according to the TID information, in **Colombia**, interception powers in such times are the same as under the law in times of peace;

the only special power is the power of the authorities to demand priority access to communication services in emergencies.

In the **USA**, the President can declare a "national emergency" and then claim certain exceptional powers, otherwise largely limited to times of war. Such an emergency was, in fact, declared in response to the "9/11" attacks; and that *this declared state of emergency formally remains in effect.*[111] However, the President did not need to rely on this declaration to issue Executive Order 12333 which, as we have seen, is the main basis for the bulk interception of "international communications", because he had the power to issue that order under the President's "inherent authority" under Article II of the Constitution to conduct foreign intelligence.

Thus, neither in the **USA** nor in the other countries surveyed should we focus on special powers in formal emergencies. Rather, the worrying matter is that in the fight against terrorism, special powers departing from the "normal" rule of law have increasingly crept into the "normal" legal systems. This is not new; As far back as 1980, Amnesty International warned of the creation by anti-terrorism legislation of "semi-permanent quasi-emergencies".[112] This remains the danger: that special powers, which would "normally" be regarded as unacceptable, are put on the statute book to counter the "special" threats posed by serious terrorists, and then remain there, and are slowly extended to other areas of concern, such as organised crime to "economic threats", "cybercrime" and acts threatening "cybersecurity", and "extremism". This is well illustrated in this report by the contrast between the "normal" powers of targeted lawful interception of communications by law enforcement agencies, on the basis of a judicial warrant, and the "generic access" now increasingly granted to the security services to communications, and communications infrastructure, without judicial authorisation or adequate oversight.

2.3.6 Secret "Extralegal" Operations

Although this report must focus on the use of lawfully granted powers, we cannot ignore the fact that surveillance also appears to be carried out in the absence of legal authority, or under secret interpretations of the law that no ordinary person could have foreseen.

We have already noted that some of the core programmes of the **USA**, exposed by Edward Snowden, relied on secret interpretations of the law that would never have been revealed had it not been for his revelations; and that the same applies to much of the **UK**'s GCHQ's activities. Indeed, it is clear that much is still being done by the NSA and GCHQ that is kept secret (or as secret as the authorities can manage in the light of the exposures) in legal frameworks that are so opaque that they cannot be regarded as "law" in terms of international human rights law. These programmes are therefore ipso facto in breach of the International Covenant on Civil and Political Rights and the European Convention on Human Rights. This has already been effectively confirmed by the Court of Justice of the EU, and even more explicitly by the Irish High Court, in the case brought by Austrian law student and activist Max Schrems.

But unlawful or quasi-lawful ("extralegal") surveillance operations have also been revealed elsewhere. Without trying to be comprehensive, below we provide information on some such cases.

Privacy International reports with regard to **Colombia** that:[113]
[Although] the Colombian government has reformed its surveillance laws, interrogated its technical capabilities, and even disbanded one of its security agencies in light of revelations about the abuse of surveillance systems...confidential documents and testimonies show that [these] recent reforms have been undermined by surreptitious deployment of mass, automated communications surveillance systems by several government agencies outside the realm of what is proscribed by Colombia's flawed intelligence laws.

PI commented about **Egypt's** "culture of impunity for unlawful surveillance, which is still in place in the post-Mubarak-era", and reported that:[114]
Whilst the agencies are given broad powers to carry out surveillance, the Telecommunications Act nonetheless requires a warrant for some surveillance activities; however, this requirement is not practically enforced.

In **France**, the journal *l'Obs* reported in July 2015 that both the previous and the current president had authorised the "top secret" tapping into the undersea global communication cables that land in France. Apparently, the surveillance was based on a secret decree of 2008, later linked to an also secret annexe to the 2010 French/British Lancaster House Agreement on defence cooperation. After this was revealed, the practice, instead of being halted, was legalised in the recent (1 October 2015) International Surveillance Law.[115]

In **Germany**, it was reported not only that the BND had relied on "creative" interpretations of the law to carry out surveillance beyond what most lawyers thought was lawful, even within the country, but also that it had refused to give information on broader programmes involving the extensive "tapping into" of the global fibre-optic communication cables, under such headings as "Monkeyshoulder" and "Wharpdrive", in very close cooperation with the **US**'s NSA.[116] This tapping resulted in the collection of some 220 million datasets each day, of which some two million were retained indefinitely.[117]

With regard to **Kenya**, Privacy International noted that although the law requires judicial approval for the interception of communications, "there are concerns that judicial processes are being circumvented and the privacy of citizens violated."[118] It also noted that:[119]
Vodafone's transparency report, Law Enforcement Disclosure Report, published in June 2014, revealed that it had "not received any agency or authority demands for lawful interception assistance" in Kenya. The inference from this disclosure is that the Kenyan authorities have direct access to Vodafone's network, which allows the government to monitor communications directly without having to go to the company to seek the data of their customers.

On **Myanmar**, Privacy International noted that it was altogether "unclear under what legal regime [the various intelligence agencies] are operating, with what remit and powers, and how their policies and practices adhere to international human rights obligations to protect the rights to privacy and freedom of expression."[120] Of Pakistan it said that "Interception across Pakistani networks is pervasive; some of it is also unlawful."[121]

On **South Africa,** Privacy International reported that: [122]
Despite the aim of RICA [the Regulation of Interception of Communications and Provision of Communications Related Information Act]

to regulate the interception of communications, there have been consistent reports of state surveillance being carried out outside the RICA legal framework, in manners that violate the right to privacy. This is particularly so with regards to the National Communications Centre (NCC), the government's national facility for intercepting and collecting electronic signals on behalf of intelligence and security services in South Africa. It includes the collection and analysis of foreign signals (communication that emanates from outside the borders of South Africa or passes through or ends in South Africa).

The capacity of the NCC to conduct unregulated mass surveillance was highlighted by the Mail & Guardian in 2013. The report noted how the agency is able to conduct mass monitoring of telecommunications, including conversations, emails, text messages and data, without judicial authorisations or other safeguards.

A Ministerial Review Commission on Intelligence in South Africa (known as "Matthews Commission") set up to review intelligence gathering in South Africa found that the NCC carries out surveillance (including mass interception of communications) that is unlawful and unconstitutional, because it fails to comply with the requirements of RICA.

The Matthews Commission report, released in 2008, made a series of recommendations to address the lack of control and regulations of the South African intelligence agencies. These recommendations have, by and large, not yet been acted upon by the government.

In **Turkey**, the law itself is so lax as to effectively allow for unrestrained surveillance, blurring the lines between legal and extralegal activities:[123] **Turkey's laws in general fail to enshrine any clear limitations on the scope of retention and access to private data. The new MİT law fundamentally undermines the right to privacy by permitting the agency unfettered access to data without judicial oversight or review.**

Furthermore, the new law permits the agency to "collect data relating to external intelligence, national defense, terrorism, international crimes and cyber security passing via telecommunication channels" without specifying the need for a court order. Beyond this measure, with the authorization of the head of agency or deputy heads, the law gives the intelligence agency the authority to intercept calls overseas, and calls by foreigners and pay phones, and analyze and store the data.

In practice, much the same can be said of **Russia** (see section 4.10). Overall, therefore, the sad conclusion must be that in the vast majority of countries surveyed, either the law effectively provided no real limitations on surveillance, or the security agencies still carry out indiscriminate surveillance, regardless of the law.

4
Overview of the Cases

4.1 Colombia

The 1991 Colombian Constitution guarantees the right to privacy and confidentiality of communications. However, the Colombian Criminal Procedure Code allows for targeted lawful interception of communications without judicial authorisation, on the order of officials from the *Fiscalia*, headed by the Attorney General (the equivalent of *procurators* or public prosecutors in other countries). The military, the police, and the intelligence services may, with judicial authorisation, intercept private telecommunications for the purposes of national security, even where they are not investigating a specific crime. However, the safeguard of judicial authorisation in this context is undermined by the fact that, under Decree 1704 of 2012, TSPs and (M)NOs may be required to install technical equipment to facilitate interception and monitoring; and various agencies may access the TSPs and (M)NOs networks via these officially mandated "connection and access points" (Constitutional Court Decision C-594 of 2014). It seems likely that these connection and access points amount to what is known in surveillance studies as a "back door".

Even these broad legal surveillance powers do not mean that the law is always observed and there have been numerous documented surveillance scandals. Privacy International has noted that law enforcement agencies from the Administrative Department of Security to the Army to the Police Intelligence Directorate have been implicated in the unlawful targeted surveillance of journalists, activists and government actors. As Privacy International put it, in Colombia, "An overly broad, technically unsound legal framework enables interception of communications to occur without adequate safeguards."[127] The publication, by TSPs, of aggregate data on the use of interception powers (in relation to both metadata and content) can be prohibited – and the absence of any such data suggests this power could have been used.

4.2 DR Congo

The 2005 Constitution of the DR Congo guarantees the right to privacy and confidentiality of communications. However, powers for law enforcement investigations under the 2002 Telecommunications Framework Law are sweeping and do not require judicial authorisation for targeted interception; authorisations for such LI can be granted by the Attorney General. Under the same law, the police and intelligence agencies can carry out untargeted interceptions of both metadata and content for "national security, protection of the essential elements of the scientific, economic and cultural potential of the country, or the prevention of crime and organised crime", on order of the Minister of the Interior, without judicial authorisation. In fact, the law is so sweeping that it should be assumed the authorities can also demand the installation of "back doors" under its vague provisions. There is effectively no independent oversight over the use of the above-mentioned powers.

Due to weak rule of law and adherence to due process in the DR Congo, legal provisions are not always a constraint on surveillance. It is unclear whether direct access has taken place under the vague powers that presently exist.

4.3 Egypt

The 2014 Egyptian Constitution guarantees the right to privacy and confidentiality, including that of communications. However, under the Criminal Procedure Code, access to both metadata and content can be ordered as part of ordinary criminal investigations, with either a prosecutor's or a judge's authorisation. Further, the armed forces, police, intelligence services, and the administrative control authority have broad and ill-defined powers to obtain metadata and content in relation to national security concerns, under the 2003 Communications Law. "National security" is undefined in this context. The same law grants authorities the power to assume access to TSPs and MNOs infrastructure, without either being able to check how this access is used, thus in effect allowing the installation of "back doors". Additionally, provision 31 of the 2014 Egyptian Constitution allows for the protection of cyber assets, as part of the economy and national security, that can also be used for surveillance. There is no independent oversight over the use of the above-mentioned powers, save for court orders that are theoretically required but are almost never made public.

A new Cybercrime Law, drafted in secrecy but the existence of which was disclosed in April 2015, was reported as having been adopted but still requiring executive approval. Reports suggest the unpublished law will "codify many of the surveillance and Internet-related 'security' practices that have become routine within the current government." [128]

Importantly, adherence to rule of law in Egypt, which was already poor under previous regimes, has deteriorated even further. The existing justice system cannot be seen to be impartial and is heavily influenced by political decisions. Moreover, military tribunals, appointed and overruled by the defence minister, are likely to look into national security cases. It is unclear whether governments are using their "emergency" powers to take control of infrastructure to facilitate direct access to telecommunications provider infrastructure. These emergency powers were used to facilitate the infamous disconnection of communications in Egypt during the Arab Uprisings in 2011. The requirement that a judicial warrant is obtained for at least some surveillance activities is not practically enforced; and overall there is still "a culture of impunity for unlawful surveillance."[129]

4.4 France

In France, there is no specific constitutional right to privacy or confidentiality of communications. However, this right is provided for in other laws (in particular the Civil Code and the Code on the Mail and Electronic Communications, CMEC), and through the (somewhat complex) domestic application of the European Convention on Human Rights in domestic law. Metadata access in targeted criminal investigations can be authorised under the Criminal Procedure Code by either a prosecutor or a judge—more specifically, the investigative judge (juge d'instruction) acting in a criminal investigation. Under CMEC, too, access to communications content must be ordered by a judge.

The recent Law on Surveillance over International Communications, adopted on 1 October 2015, allows for generic access to "international" (i.e., "external") communications data on the order of the Prime Minister (without judicial involvement) for the purposes not just of defending the nation or the prevention of terrorism but also in support of "major foreign policy and economic, industrial and scientific interests" of the state.

Article L. 34-1-II of the CMEC furthermore requires TSPs and (M)NOs to "implement relevant internal processes" to "respond to requests for access" to data – which suggests that there is some control by the TSPs and (M)NOs over the responses to those "requests" from the authorities. But in practice, this mandatory "assistance" may well lead to direct access to the data without the knowledge or involvement of the TSPs and (M)N, i.e., by means of "back doors".

The use of the generic access powers provided for in the recent law is only subject to "advice" from various bodies, not real oversight. The October 2015 law furthermore contains a provision which allows for secret decrees by the Conseil d'État to regulate the detail of the relevant surveillance (Article L. 854-1), raising concern about secret, excessively broad interpretations of the law. There are no statistics available yet on the use of these powers, but there have been revelations about extensive illegal surveillance before the law was adopted. Indeed, the law appears to have been adopted specifically to legalise practices retrospectively that were clearly unlawful before its adoption.

Thus, the journal l'Obs reported in July 2015 that both the previous and the current president had authorised the top secret tapping of undersea global communication cables entering France. Apparently, the surveillance was based on a secret decree of 2008, later linked to a secret annex to the 2010 French-British Lancaster House Agreement on defence cooperation. After this was revealed, as just noted, the practice, instead of being halted, was legalised in the October 2015 law.

4.5 Germany

The German Constitution, the "Basic Law" (*Grundgesetz*), grants strong protection to the right to privacy and confidentiality of communications and data protection. Quite different legal regimes apply, however, for surveillance by law enforcement as opposed to intelligence services.

In criminal matters, a Lawful Intercept Order may only be issued by a court at the request of the prosecutor, except in urgent cases when the prosecutor may issue the order, but in such instances the orders must be confirmed by the court within three days. The issuing of the orders is also subject to a series of other safeguards and conditions. Together with its French counterpart, the system in the German Criminal Procedure Code (StPO) is a good example of a rule-of-law-compliant system for "normal" targeted law enforcement interception and can be regarded as "best practice". Nevertheless, limited "line identification" data (who was formally assigned a specific IP address or phone number at a certain point in time) can be obtained on demand, by a wide range of authorities, and without judicial oversight even in relation to minor offences.

There are also issues in relation to generic access to communications data by intelligence agencies. The well-known "Article 10 Law" (so-called G10, named after the article of the Basic Law that guarantees the privacy of communications) allows for lawful interception and broader communication surveillance, including the "hoovering up" of data in bulk, by the intelligence services in so-called "strategic interception" of "external" or "international communications". This law is subject to some restrictions not found in other national laws, in particular that the "strategic interception" must be limited to terrorism and other serious crimes, and that "key words" used in the filtering of the bulk data must be approved by a special "G10" Commission. Under the law, TSPs and (M)NOs must "assist" in the implementation of interception, which in practice may well lead to direct access without the knowledge or involvement of the TSPs and (M)NOs, i.e., to the installation of "back doors". In addition, it has been revealed that the Intelligence Services in any case do tap directly into the main Internet and electronic communication cables running to or from and through Germany. Telecommunications surveillance by intelligence services is also exempt from judicial review. Consequently the only independent oversight is undertaken by parliamentary committees, which are understaffed for their tasks.

Although all the laws and even the technical regulations on the installation of intercept devices are published, the former in-house lawyer for the main intelligence service, the BND, has revealed that the agency relied on "creative" interpretations of the law to carry out surveillance operations, including the tapping into the global communication systems, in ways that lawyers had until then be assumed to be unlawful. Apparently detailed statistical data are published by the authorities on both targeted and untargeted ("strategic") surveillance. It was also revealed that the agency refused to give information on broader programmes involving extensive "tapping into" of the global fibre-optic communication cables to the parliamentary committee of inquiry into surveillance.

The original German Basic Law, as adopted after the Second World War, did not refer expressly to states of emergency, as the occupying powers reserved for themselves the right to intervene in such cases. But in 1968, against much popular protest, the legislator adopted "Emergency Laws"

(Notstandsgesetze) under which some otherwise constitutionally guaranteed rights—including the right to confidentiality of communications—can be temporarily suspended. To this day these broad authorities have never been used.

4.6 India

The right to privacy and confidentiality of communications is not expressly guaranteed in the Indian Constitution. There has been considerable discussion in judicial and legislative circles on whether it can be read into Article 21 of the Constitution which guarantees the right to life and personal liberty. However, the judiciary is reluctant to do so explicitly because it feels the concept is too broad and moral-based (rather than law-based). It is therefore addressed, if at all, on a case-by-case basis.

Provisions in the Indian Criminal Procedure Code on targeted lawful intercepts are sweeping and do not require judicial authorisation. The Information Technology Act, read together with the Indian Telegraph Rules, grants even wider powers to a variety of authorised government officials to intercept or monitor information transmitted, generated, received, or stored in any computer. Beyond that, there are exceptional emergency powers set out in the Information Technology Act and the Indian Telegraph Rules that can be invoked, not just when there is an actual emergency, but also "in the interests of friendly relations with foreign states" and "to prevent incitement to commit [any] offences". These provisions grant sweeping powers to order interception of whole classes of messages; on whole classes of persons; and it would seem in relation to any [specified] subject. In effect, these rules allow for arbitrary, "generic" interception of communications. The licenses under which TSPs and (M)NOs operate furthermore require these providers to make detailed communications information (both metadata and content) available to the authorities in real time—suggesting, again, the compulsory installation of "back doors".

Surveillance oversight is only by a "review committee" made up of high officials, but by law the committee must maintain utmost secrecy and destroy its own files after six months. There are evidently subsidiary rules and instruments and internal guidance on, and interpretations of, the primary rules, but these are kept secret, and/or applied arbitrarily.

Many constitutional rights can be suspended in times of "national emergency". However, given that confidentiality of communications already attracts only very little, if any, protection under the Constitution, this makes little difference in that regard.

4.7 Kenya

Subject to Article 24 on the limitations to fundamental rights, the right to privacy and confidentiality of communications is guaranteed in the 2010 Kenyan Constitution. However, a range of Kenyan laws including the National Intelligence Service Act, the Prevention of Terrorism Act, and the Kenyan Information and Communications Act provide for sweeping powers to intercept communications (both metadata and contents) without judicial order. The National Intelligence Services Act furthermore allows interception and monitoring, without targeting of any kind, to protect national security. "National security" is defined in Article 238(1) of the Constitution to include any "na-

tional interest". A judicial warrant is required for such intercepts and monitoring, but given this sweeping definition of "national security" and the absence of any substantive limitations, the procedural safeguard cannot be regarded as effective. Moreover, the National Intelligence Service Act also requires the installation of devices allowing direct access, i.e., of "back doors".

Although there is some provision for judicial authorisations and a parliamentary committee that nominally has powers of oversight over surveillance, the Kenyan legal system is weak and it is suspected that these safeguards are widely circumvented.

Moreover, as reported by Privacy International,[130] after at least 64 people were killed in two attacks by Al Shabaab militants in late 2014, members of the ruling Jubilee Coalition moved swiftly to introduce an omnibus bill, the Security Laws (Amendment) Bill 2014. The bill, which was hastily enacted into law despite street protests and skirmishes inside Parliament, curtails a spate of constitutionally protected rights while consolidating law enforcement agencies' powers to enhance Kenya's "ability to detect, monitor and eliminate security threats," in President Uhuru Kenyatta's words. Specifically, it weakens the legal safeguards pertaining to the interception of communications by police, increases the purposes for which surveillance may be undertaken, and provides for broad powers for the otherwise undefined "National Security Organs" to intercept communications.

4.8 Myanmar

The right to privacy and confidentiality of communications is guaranteed in Article 357 of the 2008 Myanmar Constitution. That constitution, however, is highly ambiguous about the true scope and effect of the rights it grants and the limitations that can be imposed on them, so the practical meaning of the guarantee is therefore minimal.

The legal framework for lawful intercepts, even in ordinary criminal investigations, is unclear to say the least, although regulations are apparently being drafted. In any case, the 2013 Telecommunications Law (and indeed, Myanmar law generally) does not contain any rules on the protection of individual privacy,[131] and allows generic interception not only when the security of the State or the rule of law is adversely affected, but also on a number of broadly stated grounds, including when it is simply "in the public interest". Furthermore, the licenses under which TSPs and (M)NOs operate contain broad requirements of technical cooperation with interception demands that can be read as allowing the imposition of effectively any condition on the service providers, including allowing the installation of "back doors".

There is effectively no independent oversight over the use of these "generic access" powers, even in normal times (the powers of the authorities in times of war or official national emergencies are essentially discretionary).

In line with the above, Privacy International has observed that it is altogether "unclear under what legal regime [the various intelligence agencies] are operating, with what remit and powers, and how their policies and practices adhere to international human rights obligations to protect the rights to privacy and freedom of expression."[132] This means that arbitrary surveillance is likely to be happening.

It should be added, however, that Myanmar is in a process of fundamental reform. There is some potential that elections in 2015 will improve the current state of affairs, and provide a new draft Interception Law – but the text has not yet been released.[133]

4.9 Pakistan

The right to "privacy of the home" is guaranteed in Article 14(1) of the Pakistan Constitution (last modified in 2012). The right of access to information on a matter of public importance (which is relevant in relation to access to laws, etc.) is guaranteed under Article 19-A of the Constitution.

Interception of communications, even in relation to ordinary criminal investigation, is regulated, not in the Criminal Procedure Code or the 2002 Police Order (as one would expect), but in the Pakistan Telecommunication (Re-Organisation) Act 1996 (PTRA) which gives extremely sweeping powers of interception to a wide range of authorities, without the need for judicial authorisation. The PTRA powers can be used to gain generic access to communications data (both metadata and contents) in relation to broadly defined purposes and offences. Specifically, s. 54 of the PTRA allows the Government to authorise "any person" to intercept or trace communications, not just in cases of actual emergency but more broadly in relation to broadly defined "national security" issues or for the "apprehension of any offence". In order to conduct surveillance under the PTRA the respective agency requires a general government authorisation, currently provided to all surveillance agencies including Federal Investigation Authority (FIA) and the notorious Inter-Services Intelligence Agency, ISI.

The law also requires the installation of devices allowing the agencies direct access, i.e., "back doors". While the Investigation for Fair Trial Act 2013 requires a warrant for any surveillance of the internet or other computer system, this is simply not adhered to in actual surveillance practices. On national security issues, the government authorities just use direct access without applying for authorisation.
There is effectively no independent oversight over the use of these powers of generic access.

In accordance with Article 19-A of the Constitution, it follows from the Freedom of Information Ordinance 2002 that in principle all legal rules should be accessible (because they are information held by public authorities). However, there are broad exceptions contained in the Ordinance, in particular in relation to broadly defined national security. This suggests that certain rules relating to surveillance, in particular subsidiary rules or internal guidance and interpretations of those rules, can be kept secret. Moreover, the release of all information about interceptions, including the release of aggregate data, is expressly forbidden under the Official Secrets Act 1923 (although, of course, occasionally some information may come out in court).

4.10 Russia

The 1993 Constitution of the Russian Federation guarantees the right to privacy of correspondence, of telephone conversations, postal, telegraph, and other messages. Under the Russian Criminal Procedure Code and other laws relating to lawful intercept, the contents of communications in

ordinary criminal investigations should be allowed only in certain relatively serious cases, and subject to a judicial order issued at the request of a public prosecutor or other criminal investigation body; such lawful intercepts should be of limited duration. However, access to metadata does not require a court order. Moreover, the "National Security Concept of the Russian Federation" is set out in sweeping terms in Presidential Decree No. 24 2000. Consequently, in cases relating to national security, no suspicion or evidence of any specific criminal offence needs to be shown, meaning that if the authorities claim a national security issue is at stake, the court is given little leeway to deny the order. Under the country's Counter-Terrorism Law, the national security agency, the FSB, can "take control of private communications", and gain unrestricted access to communications data, both metadata and content. Furthermore, the "Rules on Cooperation" that set out the terms of the relationship between the TSPs and (M)NOs on the one hand, and the Intelligence Services on the other hand, can clearly allow the latter to require the installation of "back doors".

There is effectively no independent oversight over the use of the above-mentioned powers of generic access. Article 64 of the Law on Communications and Article 10.1 of the Law on Information prohibit TSPs and (M)NOs from revealing any information about any tactical or organisational actions taken or methods used by the Intelligence and Security Agencies to conduct investigations by using data from a provider or operator's network, and it would appear that this prohibition is construed so widely as to prevent the providers and operators concerned even from publishing the laws and regulations to which they are subject. They are undoubtedly barred from releasing details such as aggregate data on the use of interception warrants.

Overall, in Russia, the law itself is so lax as to allow for unrestrained surveillance, blurring the lines between legal and illegal surveillance activities.

4.11 South Africa

The 1996 South African Constitution guarantees the right to privacy and confidentiality of communications.

South African law relating to real-time lawful intercept of the contents and metadata of communications in ordinary criminal investigations requires that this should be allowed only in certain relatively serious cases, and subject to a court order, of limited duration, issued at the request of a public prosecutor or at the request of the intelligence services of the South African National Defence Force, the Crime Intelligence Division of the South African Police Service and the State Security Agency. Access to archived metadata can be ordered by any judge or magistrate.

However, under the Regulation of Interception of Communications and Provision of Communication-Related Information Act no.70 of 2002 (RICA), much wider powers of generic access to communications data (both metadata and content) are granted in relation to excessively broadly defined matters of "national security".[134] Under RICA, for metadata, authorisation can be given by a magistrate, but for communication content, authorisation must be given by a "designated" judge, which can be a retired judge. Many would regard the involvement of government-se-

lected judges as worrisome, but others feel that such judges can develop important expertise in relation to surveillance and interception of communications. Whatever that be, the requirement of a judicial authorisation is undermined by the low threshold required for authorisations.

The text of RICA is highly complex, but we were told that it does not allow the authorities to order the installation of "back doors" that would allow direct access to communications content that would not be monitored. Under the law, they should apparently always have to go through the TSPs to obtain access to communications content.

The law moreover expressly prohibits the release, by TSPs and (M)NOs, of information on the use of lawful intercept and broader "generic access" surveillance powers, including aggregate information.
Privacy International has reported serious abuses, which were not prevented by the above requirements.[135] Specifically, it noted that: "there have been consistent reports of state surveillance being carried out outside the RICA legal framework, in manners that violate the right to privacy…A Ministerial Review Commission on Intelligence in South Africa (known as 'Matthews Commission') set up to review intelligence gathering in South Africa found that the NCC carries out surveillance that is unlawful and unconstitutional, because it fails to comply with the requirements."[136]

4.12 Turkey

The 2002 Turkish Constitution guarantees the right to privacy and confidentiality of communications. Although a court order has traditionally been required for lawful interception of the content of communications under the Criminal Procedure Code, under a more recent 2014 law (technically an amendment to a 2007 Law "on regulation of publications on the internet and combating crimes by means of such publications"), the law enforcement and intelligence agencies are granted wide powers of generic access to both metadata and contents of communications in relation to excessively broadly defined matters of "national security". In particular, in an undefined set of "non-delayable" cases, interception of communications (both metadata and contents) can be ordered, also by the intelligence agencies, without a court order on grounds of "national security, public order, prevention of crime, protection of public health and public morals, protection of the rights and freedoms of others". The Information and Communication Technology Authority, BTK, can also order the interception of communications data (again, of both metadata and contents) for the purposes of protecting public safety and "public interests", after obtaining a (positive) "opinion" from the Ministry of Transport and Communications. Under the Regulation on Authorisation within the Electronic Communication Sector, the ICT Authority can also impose conditions on TSPs and (M)NOs, including technical requirements for interception, meaning that it can order them to allow the mandatory installation of "back doors".
There is no independent oversight over the use of the above-mentioned powers of generic access. According to Privacy International, there is a widespread perception in Turkey that mobile communications are monitored by state agencies on a large scale. In view of the above, it would appear that in Turkey, as in several other countries included in our survey, the law itself is so lax as that it seems to allow for unrestrained surveillance, thereby blurring the lines between legal and illegal surveillance.

4.13 United Kingdom

There is no written constitution in the UK. Instead, the rights of privacy and confidentiality of communications are protected under the Human Rights Act. Even in ordinary criminal investigations, warrants authorising lawful (targeted) interception of the contents of communications are issued (under the Regulation of Investigatory Powers Act, RIPA) by a politician (i.e., the Home Secretary), rather than by a judge. Further, access to metadata can be self-authorised by a wide range of public bodies.

Under s. 8(4) RIPA, Government ministers have sweeping powers to authorise the interception of bulk or mass data (metadata or content) from "external communications", i.e., communications that involve the transmission of data to or from the UK. This does not cover communications that take place entirely and solely within the UK, but when it comes to Internet traffic, or voice-over-Internet-protocol (VoIP) communications, those almost invariably involve the sending of data outside of the UK, even if a UK person visits a UK website, or makes a VoIP call to another person in the UK.

Moreover, a single such warrant can conceivably specify "all communications entering and leaving the British Isles". Such communications carried on a particular cable—and associated broad warrants, covering the communications of millions of individuals—may well be precisely what is required in order to carry out the kind of keyword analysis of bulk data that we now know GCHQ engages in.

The broadest of all provisions is s. 94 of the Telecommunications Act 1984. This gives the government the power to issue "directions" to providers of public electronic communications networks to do, or not to do, anything. It was long suspected that this power was used in relation to the surveillance programmes revealed by Edward Snowden, but this has only recently been formally confirmed by the government, after it had been urged to "avow" (i.e., own up to) the use of the power to gain direct, bulk access to communications data (i.e., metadata), by the official reviewer of the legislation, David Anderson QC.[137] Anderson revealed that both he and Parliament's Intelligence and Security Committee (the official oversight body over the intelligence services) had been informed of this use of the power, but had been barred from revealing it in their reports.

The various oversight commissioners are not independent, and report to the Prime Minister. The members of the parliamentary oversight committee, the ISC, are also appointed by the Prime Minister, and its reports are subject to redactions and deletions by the Prime Minister. The Investigatory Powers Tribunal has limited powers and its processes are nontransparent.

Although the primary statutes (in particular RIPA, the Telecommunications Act and the Intelligence Services Act) are published, the detailed rules governing the UK's surveillance activities under broadly phrased statutory provisions—and those governing its data sharing arrangements, in particular with the USA—were completely secret until February 2015, when the Investigatory Power Tribunal ruled that this was contrary to the Human Rights Act, following which some small, selective portions of the policies were made public. However, most of the detailed rules issued under, and interpretations of, the law remain secret. This secrecy is currently being challenged in the European Court of Human Rights by Privacy International and nine other human rights organisations.

Information on the actual use of the above powers is redacted from published official reports. Moreover, s. 19 RIPA prohibits TSPs and (M)NOs from releasing such information.

4.14 United States

The Fourth Amendment of the US Constitution protects against "unreasonable search" but is quite extensively interpreted as providing protection also of communications. However, it is limited to US nationals and lawful residents (together, "US persons") and does not extend to "non-US persons". Under the Fourth Amendment, lawful interception of the contents of communications in ordinary criminal investigations against US persons requires a judicial warrant.
Access by public authorities to metadata is generally unregulated as a result of the so-called third party doctrine, under which data that has been "voluntarily" disclosed to third parties (such as a called number that a person making a call provides to a TSP or (M)NO) no longer qualify for privacy protection.

Under FISA and the FISA Amendment Act, intelligence agencies (including the NSA) are given unlimited power to intercept in bulk, without a proper targeted judicial warrant, any "foreign" communications (i.e., communications from or to another country), provided that the communications of US persons are not specifically targeted. This applies to both metadata and content. The Snowden revelations disclosed that these powers are used by the US to "hoover up" essentially all data flowing through the undersea cables entering the country, which carry a large proportion of global Internet and other communications data, i.e., for generic access to those communications.

The US's NSA has demanded direct generic access to the systems of US TSPs and (M)NOs and globally operating US Internet Service Providers and social networks, including Google, Facebook and Apple – with the companies in question being placed under a "gagging order" which legally prevents them from informing (the data subjects (their customers anywhere in the world), of the fact that their data are directly and indiscriminately accessible to—and accessed by—the NSA. This sweeping access is further complemented by the hacking practices discussed in conjunction with UK's GCHQ.

US oversight systems do not extend to indiscriminate surveillance and generic access to "external" communications. Specifically, the Foreign Intelligence Surveillance Court (FISC), has no jurisdiction over many significant surveillance activities, including those authorised under Executive Order 12333, the main basis for bulk intercept of external communications (enacted under the President's "inherent authority" under Article II of the Constitution); and there is a near total lack of transparency about its proceedings and decisions, with extensive reliance on intelligence agencies themselves to report non-compliance. As a result, while remedies for US persons are weak, those for non-US persons are essentially illusory.

The NSA's programmes rely on secret rules and secret interpretations of the law, which cannot lawfully be reported (though some were revealed in NGO litigation).

The US Government is extremely reticent to reveal actual practices, programmes and statistics on its massive global surveillance operations. What the Snowden revelations and NGO litigation disclose is that the collected surveillance data amounts to *trillions* of datasets of *billions* of individual communications, collected and at least temporarily archived in massive NSA databases.

The President can declare a "national emergency" and then claim certain exceptional powers, otherwise largely limited to times of war – and such an emergency was in fact declared in response to the "9/11" attacks, and *formally remains in effect.*

5
Conclusion and Recommendations

Information technology has given us an unprecedented opportunity to enhance counter-terrorism and law enforcement efforts. However, these advances must not come at the expense of the core values of our society that we seek to protect. Surveillance powers as currently legislated in the 14 countries surveyed go well beyond what is necessary and proportionate. There is a danger that these powers will be extended beyond their original intent through "purpose creep"138 as different parts of governments are tempted to misuse these powers. But our fundamental freedoms and human rights need not be at odds with law enforcement; there is a way forward that balances these imperatives for the greater good.

Drawing on lessons in the case studies presented above, we have generated a set of proposed standards for the **legal foundation, transparency, accountability,** and **oversight** of surveillance powers of intelligence agencies and law enforcement. These matters are closely inter-related, and standards are therefore not easily and narrowly categorised under these headings. For example, there can be no accountability without first clarifying the legal frameworks, domestic or international, to which actors are to be held accountable. Transparency must also exist to show whether the actions of the agencies, in practice, conform to the standards set for them.

In order for there to be accountability and transparency, there must be processes and institutions with access to information that is meaningful, and reported in relevant ways. Finally, accountability and oversight must be accompanied by consequences for any failures to meet the relevant standards. These consequences should take the form of: (1) individual redress and remedies for wronged individuals; (2) disciplinary, administrative and, if appropriate, criminal sanctions imposed on wrongdoers within or by the agencies; and (3) changes to bad practices. All three forms of consequence should again be linked back to legal foundation and transparency, in that redress or punishment or corrections must themselves be known as potentialities and disclosed (at least in general terms) for general awareness. These are all elements of the rule of law.

Work on the above should be inspired by the excellent document, *Necessary and Proportionate Principles*.[139] The process to developing

these principles was led by Privacy International, Access and the Electronic Frontier Foundation and provides an excellent basis for additional conversations on how to govern government surveillance.

The standards set out at the end of our executive summary are informed by comparative constitutional and international legal requirements (particularly in terms of human rights law), and are intended to be practical to implement. It should be noted that the proposed standards are not good practices, let alone best practices, as that would require going beyond the scope of existing legal obligations within International Human Rights Law. Instead, these proposed standards are an attempt to ensure greater compliance with existing international legal obligations and can thus be regarded, at best, as **attempts to achieve a bare minimum of transparency, accountability, oversight and governance over government surveillance practices.**

Space for notes:

Endnotes

[1] http://thewebindex.org

[2] See section 1.3 on the terminology and definitions used in this report.

[3] See: Information On Country Legal Frameworks Pertaining To Freedom Of Expression And Privacy In Tele communications https://www.telecomindustrydialogue.org/resources/country-legal-frameworks

[4] See the references in notes to section 2.3 of this report.

[5] Field Marshal Montgomery of Alamein, A History of Warfare, new edition by Jane's, 1982, p. 17

[6] See: Walton, C. Empire of Secrets: British Intelligence, the Cold War and the Twilight of Empire. 2013.

[7] See: Foschepoth, J. Überwachtes Deutschland: Post- und Telefonüberwachung in der alten Bundesrepublik, 2013.

[8] For example, see Burch, J. A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and Their Implications for Homeland Security. June 2007. https://www.hsaj.org/articles/147

[9] See Korff, D."Protecting the right to privacy in the fight against terrorism", Issue Paper written for the Commissioner for Human Rights of the Council of Europe. December 2008. Available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper(2008)3

[10] On the approach of the ECtHR (which is the most developed in this regard), see: Korff, D., "The Standard Approach under Articles 8–11 ECHR and Article 2 ECHR", available at:
http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf
For more detail and full references to the ECtHR case law underpinning that summary, see the same author's Expert Opinion provided to the Committee of Inquiry into surveillance of the German Bundestag, section C.2.a, under the heading "Basic human rights principles and case-law", p. 10ff, available at:
http://www.bundestag.de/blob/282874/8f5bae2c8f01cdabd37c746f98509253/mat_a_sv-4-3_korff-pdf-data.pdf
The CJEU follows the same reasoning (leaving aside a somewhat academic difference as concerns the relationship between necessity and proportionality), especially in its more recent case law, more specifically in relation to matters of direct relevance to the present report, including compulsory data retention. For a particularly useful analysis of both the ECtHR and CJEU case law in this regard, see the opinion of the EU "Article 29 Working Party" (the body representing the data protection authorities in the EU Member States) on the application of necessity and proportionality concepts and data protection within the law enforcement sector, Opinion 01/2014, WP211, adopted on 27 February 2014, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf
On the application of essentially the same tests by the Human Rights Committee, with particular reference to Article 17 ICCPR (the right to privacy), see the statement by Martin Scheinin, former UN Special Rapporteur on human rights and counter-terrorism, to the European Parliament's LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, at its hearing on 14 October 2013, in particular points (a)–(g) on p. 3, available at:
http://www.europarl.europa.eu/document/activities/cont/201310/20131017ATT72929/20131017ATT72929EN.pdf

[11] The 2009 Annual Report of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights contains a good summary of the application of the same principles under the ACHR, by the I-A CommHR in particular (even if that report relates to the right of access to information rather than specifically to privacy): see section 7, para. 27ff, available at:
https://www.oas.org/dil/access_to_information_IACHR_guidelines.pdf

[12] Cf. the outline of the Court's approach in the freedom of expression case of Konaté v. Burkina Faso, judgment of 5 December 2014, para. 125, where the Court said that, once the case had been declared admissible, it next had to consider: "whether restrictions on the freedom of expression imposed by the Respondent State are provided by 'law', within international standards, pursue a legitimate objective and are a proportionate means to attain the objective being sought." The judgment is available at:
http://www.african-court.org/en/images/documents/Judgment/Konate%20Judgment%20Engl.pdf

[13] For example, see Scheinin, M., Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, p. 11, available at:
http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf.
See also General Comment No. 27, adopted by the Human Rights Committee under Article 40, para. 4, of the International Covenant on Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999.

[14] The summary is taken from the Expert Opinion prepared by Douwe Korff for the Committee of Inquiry of the German Bundestag (endnote 1), at p. 18. The analysis of the case law of the ECtHR underpinning the summary, with full references (in particular to the cases Klass v. Germany, Liberty & Others v. the UK, Malone v. the UK, and Weber and Saravia v. Germany) can be found on the preceeding pages (pp. 14-17).

[15] Roman Zakharov v. Russia, Application Number 47143/06, Grand Chamber judgment of 4 December 2015.

[16] Application 58170/13, 30 September 2013. The full text of the application (and of supporting documents and witness statements) is available at: https://www.privacynotprism.org.uk/news/2013/10/03/legal-challenge-to-uk-internet-surveillance/
The Court has fast-tracked the case and a judgment may, unusually, be handed out still this year.

[17] CJEU Grand Chamber Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, 8 April 2014, available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=153045&doclang=EN

[18] Grand Chamber Judgment Case C-362/14, Maximillian Schrems v. [Irish] Data Protection Commissioner, 6 October 2015, available at: para. 94.
http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=EN

[19] Note that Prof. Scheinin, in his Statement to the EP LIBE Committee (endnote 1), called upon the Human Rights Committee to issue a new General Comment on Article 17 ICCPR in the light of the Snowden revelations.

[20] Human Rights Committee, Concluding observations on the fourth periodic report of the United States of America, CCPR/C/USA/CO/4, 23 April 2014, para. 22, available at: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fUSA%2fCO%2f4&Lang=en

[21] The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, UN General Assembly, A/HRC/27/37, 30 June 2014, available at:
http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc
The report acknowledged the "major substantive contribution" to the preparation of the HCHR's report provided by a research project carried out under the auspices of the United Nations University (see para. 8). Although this study has not been published, we can confirm that it highlighted the very same basic and specific principles also adduced in the present section of this report (because one of us was a co-author of the UNU study).

[22] The rule of law on the Internet and in the wider digital world, "Issue Paper" prepared for the Commissioner for Human Rights of the Council of Europe by Douwe Korff, December 2014, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper(2014)1&Language=lanAll
The Commissioner has since released another Issue Paper, on Democratic and effective oversight of national security services, prepared by Aidan Wills, May 2015, available at: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2796355&SecMode=1&DocId=2286978&Usage=2
This focuses more on the quality of the oversight mechanisms than on substantive limitations. Thus, it recommends strong authorisation systems for "untargeted bulk surveillance", "collecting communications/metadata directly" (i.e., through so-called "back doors"), and "undertaking computer network exploitation" (i.e., state-authorised "hacking" into IT systems and devices), rather than regarding such measures as inherently contrary to the rule of law. (Recommendation 6).

[23] A number of inquiries have also been carried out, or are being carried out, at national levels in various states including the USA, Brazil, Germany and the Netherlands. However, it goes beyond the scope of the present report to also cover those.

[24] Parliamentary Assembly of the Council of Europe (PACE), Resolution 2045(2015) on Mass surveillance, adopted on 21 April 2015, available at: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21692&lang=en
The recommendations paraphrased in the text are from para. 19.
The rapporteur's report – presented as an explanatory memorandum to the draft resolution – is available at:
http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21583&lang=en
(scroll down and expand the Explanatory Memorandum by Mr Omtzigt, rapporteur).
The idea of an "intelligence codex" to cover the activities of national security agencies was first mooted at a hearing of the rapporteur in Strasbourg on 4 April 2014 by Mr Hansjörg Geiger, former head of the German national security agency the Bundesnachrichtendienst (BND) and State Secretary at the Ministry of Justice: see section 5.2 of the Explanatory Memorandum.

[25] Inter-Parliamentary Union, Resolution on Democracy in the Digital Era and the Threat to Privacy and Individual Freedoms, adopted unanimously by the 133rd IPU Assembly, Geneva, 21 October 2015, available at: http://www.ipu.org/conf-e/133/Res-1.htm

[26] Full title: European Parliament resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens, available at:
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0388+0+DOC+XML+V0//EN
For full documentation on the EP's LIBE Committee's inquiry leading up the 29 October 2015 resolution, including the texts of the working documents produced by the committee, see:
https://www.accessnow.org/policy/libe-inquiry

[27] For the full text of the principles, see: https://en.necessaryandproportionate.org/text
A list of signatories is available here: https://en.necessaryandproportionate.org/signatories
For the Background and Supporting International Legal Analysis to the Principles, see:
https://en.necessaryandproportionate.org/LegalAnalysis

[28] We will not look at the use of "signals intelligence" [SIGINT] by military agencies in times of war, if only because we found that the kinds of programmes we are concerned with do not generally rely on legal provisions covering the law of armed conflict (see section 2.3.5).

[29] The expanding of the role of the police into "preventive" action is not new. See Ian Brown & Douwe Korff, Privacy & Law Enforcement, FIPR study for the UK Information Commissioner, 2005, Paper No. 4, The legal framework, section 3.1.
The more recent developments, in particular also in relation to the blurring of the lines between policing and activities relating to national security, are noted in Douwe Korff, Protecting the right to privacy in the fight against terrorism, Issue Paper written for the Commissioner for Human Rights of the Council of Europe, 2008, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper(2008)3

[30] A page on the FBI website on "Addressing threats to the nation's cybersecurity" expressly notes that the FBI is charged both with protecting the USA's national security and with being the nation's principal law enforcement agency, adding that "[t]hese roles are complementary, as threats to the nation's cybersecurity can emanate from nation-states, terrorist organizations, and transnational criminal enterprises; with the lines between sometimes blurred." See: www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity.
The FBI has recently changed an FBI Fact Sheet to describe its "primary function" as no longer "law enforcement", but now "national security". See The Cable, 5 January 2014: http://thecable.foreignpolicy.com/posts/2014/01/05/fbi_drops_law_enforcement_as_primary_mission#sthash.4DrWhlRV.dpbs
For the dangers inherent in such blurring of the lines, see: www.foreignpolicy.com/articles/2013/11/21/the_obscure_fbi_team_that_does_the_nsa_dirty_work

[31] See Computer Weekly, "GCHQ and NCA join forces to police dark web", 9 Nov 2015. http://www.computerweekly.com/news/4500257028/GCHQ-and-NCA-join-forces-to-police-dark-web

[32] See section 1.3.

[33] The Fourth Amendment does not apply if the person affected by a "search" (which includes an online search or intercept) does not have a "significant voluntary connection with the United States" (US v. Verdugo-Urquidez, 1979). This was also confirmed to the Ad-hoc EU-US Working Group on Data Protection, established to investigate the US surveillance activities exposed by Snowden: see the Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, 27 November 2013, section 2, para. 2.

[34] Typically in a Code of Criminal Procedure, but sometimes also in Police Laws or special Laws on Special Investigative Measures (which are sometimes inserted in the criminal procedure codes [CPCs] as amendments).

[35] An exception was English law prior to 1975, under which there were effectively no common law- or statutory rules on such interception – which was found to be in breach of the European Convention on Human Rights in

the Malone case. See Nick Taylor, State Surveillance and the Right to Privacy, Surveillance & Society 1(1) (2002): 66-85, available at: http://www.surveillance-and-society.org/articles1/statesurv

[36] "Public prosecutor" is the closest equivalent to the term "procurator" in English-speaking common law countries. However, in many non-common-law countries, the office has a mandate that goes well beyond prosecutions. In many ways (especially in former socialist countries) the procurator is the general guardian of legality. In the mixed civil law/common law system in Scotland, there is the "procurator fiscal"; cf. the fiscal in Colombia. In France, she or he is called the procureur de l'etat; in Germany the Staatsanwalt; in Italy the procurore.

[37] The relevant statistics can be found here: https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung_node.html The statistics for 2014 (the most recent ones) can be found here: https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2014.pdf?__blob=publicationFile&v=2

[38] See the table in the report by Justice (the UK branch of the International Commission of Jurists), Intercept Evidence - Lifting the ban, 2006, p. 75, available at: http://2bquk8cdew6192tsu41lay8t.wpengine.netdna-cdn.com/wp-content/uploads/2015/07/Intercept-Evidence-1-October-2006.pdf Apart from in the USA, noted next in the text, the table indicates that judicial intercept warrants are also required in "normal" cases in Australia, Canada, Hong Kong, New Zealand and South Africa.

[39] Idem. According to the table mentioned in endnote 25, in Ireland intercept warrants are also issued by a politician, i.e., in that case, the Minister for Justice.

[40] For the proposal and the government's own outline, see here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf
For early criticism, in particular also of the marginal role of the proposed judicial commissioner's role, see: http://ukhumanrightsblog.com/2015/11/05/interception-authorisation-and-redress-in-the-draft-investigatory-powers-bill/

[41] See Peter Sommer, Can we separate "comm[unication]s data" and "content" – and what will it cost?, Powerpoint presentation at the FIPR event "Scrambling for Safety" (2012). https://www.cl.cam.ac.uk/~rja14/sfs-2012.html

[42] Edward Felton, Declaration in ongoing litigation brought in the US by the American Civil Liberties Union (ACLU), available at: https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf

[43] Schrems v. DPC (endnote 14), para. 93.

[44] See the report by Caspar Bowden et al. to the European Parliament, Fighting Cybercrime and Protection Privacy in the Cloud, 2012, and the subsequent article by Bowden and Judith Rauhofer, Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud, 2013, available at, respectively: http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050 http://ssrn.com/abstract=2283175

[45] Secretary of State for the Home Department v Rehman [2003] 1 AC 153.

[46] See: https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf

[47] European Parliament resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens (2015/2635(RSP)), para. 24, available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0388+0+DOC+XML+V0//EN&language=EN
The issue is of particular relevance in the EU because the Union has no competence in relation to "national security" – although it does have competences in relation to "internal security", "international security", the fight against terrorism, etc.

[48] See Douwe Korff, Expert Opinion prepared for the Committee of Inquiry of the German Bundestag into the "5EYES" global surveillance systems revealed by Edward Snowden (o.c., endnote 10), sections B.2(b), The principle of non-discrimination, and (c), The extra-territorial application of international human rights law.

[49] See Foschepoth, J. Überwachtes Deutschland: Post- und Telefonüberwachung in der alten Bundesrepublik, 2013.

[50] See again Douwe Korff, Expert Opinion prepared for the Committee of Inquiry of the German Bundestag into the "5EYES" global surveillance systems revealed by Edward Snowden (o.c., endnote 10), sections B.2(b) & (c).

[51] See sub-section 2.1.

[52] It is not impossible that these new legal powers are being introduced to address the problem that many of these countries have been widely engaged in "extralegal" activities of these kinds, often on the basis of secret laws or treaties; and that the Snowden revelations about the USA and the UK generated public outcries that would have stretched also to those programmes if they were to become known. But that is of course speculation.

[53] See: http://www.heise.de/newsticker/meldung/NSA-Ausschuss-BND-dehnt-strategische-Aufklaerungsbefugnisse-deutlich-aus-2467779.html
For further details, see the heading "transparency about the law".

[54] A back door (also referred to as a "trap door") is a means of access to a computer program that bypasses security mechanisms. See:
http://searchsecurity.techtarget.com/definition/back-door

[55] Vodafone, Law Enforcement Disclosure Report 2014, under the heading "Technical implementation of lawful interception capabilities", available at:
https://vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html#aaap

[56] Roman Zakharov v. Russia, Application Number 47143/06, Grand Chamber judgment of 4 December 2015, paras. 270 and 272.

[57] Vodafone, Law Enforcement Disclosure Report 2014, under the heading "Technical implementation of lawful interception capabilities", available at:
https://vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html#aaap

[58] See: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data -
with references to the original documents "leaked" by Edward Snowden.

[59] Independent Reviewer of Terrorism Legislation, The big reveal, 7 November 2015, available at:
https://terrorismlegislationreviewer.independent.gov.uk/the-big-reveal/

[60] Apparently, the term refers to technically trained LEA or NSA officials. They should not be confused with the French "police judiciaire" who act in relation to criminal investigations, once such investigations have been formally opened.

[61] Privacy International, The Right to Privacy in Egypt, 2014, p. 7.

[62] Quartz, You thought PRISM was bad? India's new surveillance network will make the NSA green with envy,

available at: http://qz.com/99019/no-call-email-or-text-will-be-safe-from-indias-surveillance-network/
See also: http://articles.economictimes.indiatimes.com/2013-06-28/news/40256071_1_security-agencies-telecom-service-providers-direct-electronic-provisioning
The article in the Hindu Paper referred to in the quote is here:
http://www.thehindu.com/news/national/indias-surveillance-project-may-be-as-lethal-as-prism/article4834619.ece

[63] Revealed: how US and UK spy agencies defeat internet privacy and security, Guardian, 5 September 2013, available at: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
Also: Snowden's Latest Major Leak: The NSA's Secret Campaign to Crack, Undermine Internet Security: "The NSA has secretly and successfully worked to break the widely used technology that is supposed to make it impossible to read intercepted communications", available at:
http://www.alternet.org/civil-liberties/snowdens-latest-major-leak-nsas-secret-campaign-crack-undermine-internet-security. For a detailed explanation of the technologies, see this panel discussion:
https://www.youtube.com/watch?v=oqy11TE6p7o

[64] Cf., e.g.: RFE/RL, Russian Hacking Network Found Spying On U.S., Europe For Years, claiming a group of Russian hackers known as "the Dukes" was "spying for the Russian government", see:
http://www.rferl.org/content/russia-hacking-network-spying-us-europe-dukes-fsecure/27254920.html
CNET, The wide world of hacking in China, at: http://www.cnet.com/news/the-wide-world-of-hacking-in-china/
While these reports tend to focus on hacking by Russian and Chinese hackers of Western targets, allegedly at the behest of the relevant government, for political and economic espionage purposes, it is difficult to believe that those governments would not use those same tools to carry out surveillance over their own populations, given the generally repressive approaches to dissent in Russia and China.

[65] For the USA, see, e.g., National Security Surveillance and Human Rights in a Digital Age – United States of America, Joint Submission to the United Nations Twenty Second Session of the Universal Periodic Review Working Group, Human Rights Council, April-May 2015, submitted by Brennan Center for Justice at New York University School of Law, Access, American Civil Liberties Union, Center for Democracy and Technology, Electronic Frontier Foundation, Electronic Privacy Information Center (EPIC), Human Rights Watch and PEN American Center, para. 22, available at: https://www.hrw.org/news/2014/05/01/joint-submission-re-national-security-surveillance-and-human-rights-digital-age-2015
For the UK, see, e.g., the witness statements in the case of ORG et al. v the UK (endnote 8).

[66] National Security Surveillance and Human Rights in a Digital Age – United States of America, Joint Submission to the United Nations Twenty Second Session of the Universal Periodic Review Working Group, Human Rights Council, April-May 2015, submitted by Brennan Center for Justice at New York University School of Law, Access, American Civil Liberties Union, Center for Democracy and Technology, Electronic Frontier Foundation, Electronic Privacy Information Center (EPIC), Human Rights Watch and PEN American Center, (previous note), para. 22, available at: https://www.hrw.org/news/2014/05/01/joint-submission-re-national-security-surveillance-and-human-rights-digital-age-2015.

[67] Idem, quoted in para. 24 with reference to: In re Production of Tangible Things From [REDACTED], No. BR 08-13, at 11 (FISA Ct. Mar. 2, 2009), available at https://www.aclu.org/files/assets/pub_March%202%202009%20Order%20from%20FISC.pdf

[68] Idem, para. 28.

[69] See Fundamental Rights Europe Experts (FREE), EU-US Umbrella Data Protection Agreement: Detailed analysis by Douwe Korff, available at: http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/

[70] Idem.

[71] As noted in section 4.11, not everyone feels that the use of "designated" judges is necessarily a negative aspect of the system.

[72] Privacy International, The Right to Privacy in South Africa, 2015, p. 5.

[73] See again: http://www.heise.de/newsticker/meldung/NSA-Ausschuss-BND-dehnt-strategische-Aufklaerungsbefugnisse-deutlich-aus-2467779.html

[74] Idem.

[75] As explained in sub-section 1.3, the TID information does not include the 14th country included in our survey, the USA.

[76] Roman Zakharov v. Russia, Application Number 47143/06, Grand Chamber judgment of 4 December 2015, para. 242.

[77] See, e.g.: http://www.theatlantic.com/national/archive/2012/02/the-torture-memos-10-years-later/252439/
http://www.nytimes.com/ref/international/24MEMO-GUIDE.html For the actual text of the main memorandum in this regard, see: http://nsarchive.gwu.edu/NSAEBB/NSAEBB127/02.08.01.pdf
Ius cogens, also referred to as a peremptory norm of international law, is the highest legal requirement in public international law. It cannot be set aside or overridden by treaty or other law but is binding on all states in its own right.

[78] See: EFF, What You Need to Know About the FISA Court—and How it Needs to Change, at:
https://www.eff.org/deeplinks/2014/08/what-you-need-know-about-fisa-court-and-how-it-needs-change

[79] Idem. See also: Court Reveals 'Secret Interpretation' Of The Patriot Act, Allowing NSA To Collect All Phone Call Data, at: https://www.techdirt.com/articles/20130917/13395324556/court-reveals-secret-interpretation-patriot-act-allowing-nsa-to-collect-all-phone-call-data.shtml

[80] 10 Human Rights Organisations v. the UK. The text of the application is available here:
https://www.privacyinternational.org/sites/default/files/HR%20Orgs%20v%20UK.pdf

[81] The article stipulates, inter alia, that "a not-published decree of the Council of State, adopted after having obtained the opinion of the National Commission of Supervision over Intelligence Techniques and submitted to the Parliamentary Intelligence Committee, clarifies [F: précise] the manner of implementation [F: les modalités de mise en œuvre] of the surveillance [authorised by the Law]."

[82] Amnesty International (France), Ligue des Droits de l'Homme, Syndicat des Avocats de France, Syndicat de la Magistrature, and two others, Observations Sur La Loi Relative Au Renseignement, July 2015, available at:
http://www.ldh-france.org/wp-content/uploads/2015/07/Observations-sur-la-loi-relative-au-renseignement.pdf

[83] Parliamentary Assembly of the Council of Europe, Resolution on Mass Surveillance (Resolution 2045(2015)), adopted on 21 April 2015, available at: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21692

[84] Privacy International, Tipping the scales: Security & surveillance in Pakistan, 2015.

[85] Roman Zakharov v. Russia, Application Number 47143/06, Grand Chamber judgment of 4 December 2015. para. 194

[86] We were informed that in 26 of the 47 countries included in the 2015 transparency reports of Vodafone Group, Telenor Group and Orange, the law either prohibited disclosure of the number of demands for lawful interception

and/or communications data or the law was unclear and the company was awaiting or unable to obtain guidance from the authorities.

[87] Telenor, Authority Requests for Access to Electronic Communication - Country Data, May 2015, entry on Telenor Myanmar (p. 7), available at: http://www.telenor.com/wp-content/uploads/2015/05/Authority-requests-for-access-to-electronic-communication_04.pdf

[88] Telenor, Authority Requests For Access To Electronic Communication – Legal Overview, May 2015, entry on Myanmar (p. 31), available at: http://www.telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf

[89] Vodafone says that it does not publish statistics where governments do so. However, they could (if allowed under the law) still comment on them and add their own perspective, e.g., as to the scope of the warrants.

[90] UK Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework, HC 1075, 12 March 2015, para. 41, p. 20, footnote omitted; emphasis added. The report is available at: http://fas.org/irp/world/uk/isc-privacy.pdf

[91] Idem, para. 134, at i), on p. 49, footnotes omitted.

[92] Idem, at iii), iv) and v), on pp. 49 and 50, footnotes omitted.

[93] Unterrichtung durch das Parlamentarische Kontrollgremium (PKGr) – Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 dieses Gesetzes (Berichtszeitraum 1. Januar bis 31. Dezember 2011), Bundestag document 17/12773 of 14 March 2013, available at: http://dip21.bundestag.de/dip21/btd/17/127/1712773.pdf The statistics can be found in section III.2, on pp. 4-5.

[94] Idem, section IV.2, on pp. 6-7.

[95] Idem, p. 7.

[96] BND speichert 220 Millionen Telefondaten – jeden Tag, die Zeit, 30 January 2015, available at: http://www.zeit.de/digital/datenschutz/2015-01/bnd-nsa-metadaten-ueberwachung

[97] Idem, p. 8.

[98] Fourth Periodic Report of the United States of America to the United Nations Committee on Human Rights Concerning the International Covenant on Civil and Political Rights, 30 December 2011, paras. 321-335, available at: http://www.state.gov/j/drl/rls/179781.htm

[99] United States Foreign Intelligence Surveillance Court, Washington D.C., Exhibit C, Memorandum of Law in support of Application for certain Tangible Things for Investigations to Protect against International Terrorism, p. 3, obtained in other litigation by the ACLU, available here: https://www.aclu.org/files/assets/Production%20to%20Congress%20of%20a%20May%2023,%202006%20Government%20Memorandum%20of%20Law.pdf

[100] Idem, p. 8, at D. Original italics; emphases in bold added.

[101] Cf. the references to the need for authorisation of access to content relating to communications of "US persons" in the attachment containing a document entitled "USSID 18 – Legal Compliance and Minimization Procedures (U)", on p. 3 of that document. All the limitations listed are aimed at weeding out most (not all) communications of "US persons". No such weeding out is even suggested in relation to "non-US persons".

[102] National Security Surveillance and Human Rights in a Digital Age – United States of America, endnote 53.

[103] Idem, para. 16, footnote references omitted.

[104] The discussions of the NSA's storage capacity have focussed on its special, large facility in Utah, the existence of which was revealed in 2012. See: "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)", available at:http://www.wired.com/2012/03/ff_nsadatacenter/
Estimates have included some extremely high figures of a storage capacity ranging from "yottabytes" (in Wired) to "5 zettabytes" (on NPR). The lowest quoted capacity that we have found is still "less than 3 exabytes of data capacity for the facility", with one exabyte being 1 000 000 000 000 000 000 Bytes. Our reference to "trillions" of datasets is therefore extremely low, probably by a factor of thousands.
See: http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/
On the meaning of the other terms, see:
http://highscalability.com/blog/2012/9/11/how-big-is-a-petabyte-exabyte-zettabyte-or-a-yottabyte.html

[105] Vodafone, Law Enforcement Disclosure Report 2014, under the heading "Who should publish: governments or operators?", available at: https://vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html#aaap

[106] Idem, under the heading "What statistics should be reported: warrants or targets?"

[107] Jemima Stratford QC, Advice In the Matter of State Surveillance, 22 January 2014, paras. 13-15, available at: http://www.brickcourt.co.uk/news-attachments/APPG_Final_(2).pdf

[108] Note that the International Covenant on Civil and Political Rights expressly requires that a state of emergency is formally declared before a state-party can rely on the "derogation clause" (Article 4(1)). This is also required under principle 42 of the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, drafted by the International Commission of Jurists, but endorsed by the United Nations Economic and Social Council (UN Document E/CN.4/1985/4, Annex (1985), available at: https://www1.umn.edu/humanrts/instree/siracusaprinciples.html

[109] For very useful country summaries of emergency laws and powers, see: https://en.wikipedia.org/wiki/State_of_emergency. These include, of the 14 countries included in the present report: Egypt, France, Germany, India, Pakistan, South Africa, Turkey, the UK and the USA.

[110] Note that historically, before the French Revolution of 1789, the "state of siege" was a matter of fact: a town was in a state of siege when it was cut off from the rest of the country by surrounding enemy troops; and in those circumstances the civil powers were transferred to the military authorities. However, after the Revolution, a practice took root under which such transfers were also ordered in relation to other disturbances, e.g., in relation to workers' uprisings. See: https://fr.wikipedia.org/wiki/%C3%89tat_de_si%C3%A8ge_(France)

[111] See: Special Report: America's perpetual state of emergency, available at: http://www.usatoday.com/story/news/politics/2014/10/22/president-obama-states-of-emergency/16851775/

[112] Submission by Amnesty International to a conference of the Parliamentary Assembly of the Council of Europe on "Defence of Democracy against Terrorism in Europe: Tasks and Problems", presented by Douwe Korff as Head of Europe Region of AI, 12-14 November 1980, Council of Europe Document AS/Pol/Coll/Terr(32)26.

[113] Privacy International Special Report, Shadow State: Surveillance, Law and Order in Colombia, August 2015, Executive Summary, p. 7.

[114] Privacy International and others, The Right to Privacy in Egypt, 2014., pp. 7 and 10.

[115] l'Obs, Exclusif: Comment la France (aussi) écoute la monde, 1 July 2015, available at: http://tempsreel.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html

[116] Angezapfte Glasfasern: BND und Kanzleramt verschweigen zehn weitere Operationen zur Internet-Überwachung, Netzpolitik, 5 June 2015, available at: https://netzpolitik.org/2015/angezapfte-glasfasern-bnd-und-kanzleramt-verschweigen-zehn-weitere-internet-abschnorchel-aktionen/

[117] National Security Surveillance and Human Rights in a Digital Age – United States of America, Joint Submission to the United Nations Twenty Second Session of the Universal Periodic Review Working Group, Human Rights Council, April-May 2015, submitted by Brennan Center for Justice at New York University School of Law, Access, American Civil Liberties Union, Center for Democracy and Technology, Electronic Frontier Foundation, Electronic Privacy Information Center (EPIC), Human Rights Watch and PEN American Center, available at: https://www.hrw.org/news/2014/05/01/joint-submission-re-national-security-surveillance-and-human-rights-digital-age-2015.

[118] Privacy International, The right to privacy in Kenya, 23 June 2014. https://www.privacyinternational.org/node/386

[119] Idem. In a comment on this quote, Vodafone told us that "a number of countries" had not actually installed the technical equipment that the law allows them to instal – and that in those circumstances there might therefore not be such "back door" access. However, it did not say that this was the case in Kenya, and we feel that in the circumstances Privacy International's inference remains reasonable.

[120] Privacy International, The right to privacy in Myanmar, 2015.

[121] Privacy International, Tipping the scales: Security & surveillance in Pakistan, 2015.

[122] Privacy International, The right to privacy in South Africa, 2015, with reference to Mail & Guardian, "Spy wars: South Africa is not innocent", 21 June 2013, available at:
http://mg.co.za/article/2013-06-21-00-spy-wars-south-africa-is-not-innocent
And also, "Secret state: How the government spies on you", 14 Oct 2011. available at:
http://mg.co.za/article/2011-10-14-secret-state/

[123] Privacy International, The right to privacy in Turkey, 2015.

[124] Hans Born, Ian Leigh, Aidan Wills, Making International Intelligence Cooperation Accountable, study for the Norwegian Parliament, 2015, p. 1.

[125] See Bures, O. 2012. "Informal Counterterrorism Arrangements in Europe: Beauty by Variety or Duplicity by Abundance?" Cooperation and Conflict 47 (4): 495–518. doi:10.1177/0010836712462774.

[126] See Rudner, Martin. 2004. "Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism." International Journal of Intelligence and CounterIntelligence 17 (2): 193–230. doi:10.1080/08850600490274890, page 211. For further information see SEPPER, ELIZABETH. 2010. "Democracy, Human Rights, and Intelligence Sharing." Texas International Law Journal 46 (151): 151–207 and Shpiro, Shlomo. 2001. "The Communication of Mutual Security?: Frameworks for European-Mediterranean Intelligence Sharing."

[127] Privacy International Special Report, Shadow State: Surveillance, Law and Order in Colombia, August 2015, p. 16.

[128] The Spring of Cybercrime Laws, Netizen Report, 22 April 2015, available at: http://www.slate.com/blogs/future_tense/2015/04/22/netizen_report_egypt_tanzania_and_pakistan_consider_new_cybercrime_laws.html

[129] Privacy International, The Right to Privacy in Egypt, 2014, p. 7.

[130] See: https://www.privacyinternational.org/node/99

[131] See Andrea Calderaro, Internet Governance Capacity Building in Post-Authoritarian Contexts. Telecom Reform and Human Rights in Myanmar (May 1, 2015). Available at SSRN: http://ssrn.com/abstract=2686095 or http://dx.doi.org/10.2139/ssrn.2686095

[132] Privacy International, The Right to Privacy in Myanmar, 2015, para. 30.

[133] See Andrea Calderaro, Internet Governance Capacity Building in Post-Authoritarian Contexts. Telecom Reform and Human Rights in Myanmar.

[134] See the discussion of "national security" and the Johannesburg Principles in section 2.3.

[135] Privacy International, The Right to Privacy in South Africa, 2015, p. 3.

[136] Ibid, p. 5.

[137] Independent Reviewer of Terrorism Legislation, The big reveal, 7 November 2015, available at:
https://terrorismlegislationreviewer.independent.gov.uk/the-big-reveal/

[138] http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf

[139] See International Principles on the Application of Human Rights to Communications Surveillance, May 2014.
https://en.necessaryandproportionate.org/