Human rights actors in the digital information ecosystem

Submitted by **Ahreum Lee**

Association Human Rights Officer, Office of the High Commissioner for Human Rights

(ahreumlee@ohchr.org; ahreumlee223@gmail.com)

This report is submitted pursuant to section 5 of ST/AI/2015/5, upon completion of the 2016 United Nations Sabbatical Programme.

CONTENTS

Abstract

No clear definition or agreed normative framework allows us to identify actors and ascertain who has international legal personality. The debate on subjects of international law reflects the historical origin and development of international law, which has evolved in response to changes in society. The needs of the digital information society have led to the creation of new actors, such as technical standardization entities, who participate alongside business entities in quasi-legal decision-making processes that impact the behaviour of users through their control over the flow of digital information.

The rise of non-State actors has changed society, nationally and internationally, in ways that are increasingly recognized. However, in the absence of an agreed normative approach, efforts to determine the subjects of international law often involve circular reasoning and do not offer concrete solutions. This study adopts a descriptive approach. It identifies all the relevant actors who participate in the digital information ecosystem, in terms of their functions and the actual operation of the information ecosystem. A functional approach is justified because it makes it possible to identify actors in relation to core components of the digital information ecosystem which are necessary for its operation. Core components include: provision of products and services (equipment and devices, software networks, cloud services); using the ecosystem; allocation of resources (such as frequencies and Internet domain names); creation of technical standards used in the different layers of the ecosystem; and creation of laws and non-laws that regulate actors' behaviour. An analysis of activities clearly reveals the extent to which non-State actors, including individuals, have fulfilled functions and contributed to the development of the digital information ecosystem.

Identifying actors of international human rights law does not equate to listing *all* the actors in the ecosystem. To determine which actors have the status of actors in international human rights law, it is proposed to assess the impact of functions on the enjoyment of rights. The main threats to human rights online are associated with the flow of digital information and its life cycle. By examining the capacity of each component of the ecosystem to control the flow of digital information, and identifying the actors responsible for each component, we can discern which components have an impact on human rights and which actors in the ecosystem harm (or protect) human rights. It is proposed that States recognize human rights actors in the ecosystem that have the capacity to threaten (or promote) enjoyment of human rights and establish safeguards to make sure that those actors respect human rights standards.

If an actor in the digital ecosystem acquires the status a human rights actor because it fulfils certain functions, this does not necessarily imply that it has legitimate authority to carry out those

functions. Several questions and concerns arise with regard to the legitimacy of human rights actors that *de facto* exercise critical functions in the digital information ecosystem. To resolve issues of legitimacy, it is suggested that States should recognize human rights actors in the digital information ecosystem as actors having obligations under international human rights law. It is also suggested that human rights actors in the digital information ecosystem must themselves claim and implement their human rights obligations so that they can carry out their functions avoiding central regulation. Their legitimacy, as well as the sustainability of the ecosystem, depends on this.

The dynamic nature of the digital information ecosystem and the way it has evolved with little State involvement has created a new typology of human rights actors. These actors are trans-governmental institutions composed of: public authorities (such as regulatory authorities) that are part of government but do not necessarily have the authority to make law; international (Internet) institutions that have evolved organically to resolve problems and whose aim is to expand the Internet; international agencies (established by international organizations) and multi-stakeholder platforms; and industry associations with the status of NGOs. States should recognize these entities as human rights actors; individual rights holders should be aware of these new human rights actors, the functions they fulfil, and the impact of those functions on personal rights.

The digital information ecosystem changes rapidly under the influence of new technologies. The functions that are core to the digital ecosystem both promote and curtail individual rights, by controlling the flow of digital information. As new technologies emerge, they will influence the organization of the digital ecosystem, including the content of its core functions, and may pose new threats to the enjoyment of rights. This means that new human rights actors may also emerge. The core functions of the digital ecosystem are static and stable but they are complicated to understand for people without technical knowledge. By contrast, (human rights) actors in the digital ecosystem are prone to change. For this reason, all human rights actors in the digital information ecosystem need to know who does what in the digital ecosystem, and how their roles are evolving, in order to discern how best to protect human rights. New categories of human rights actors may emerge and all human rights actors, including individual rights holders, need to be aware of the functions they undertake, and the impact of those functions on rights.

This report starts by examining the subjects of international law in the historical context of the international legal system (section 2.1). Having noted that the international normative legal framework does not adequately provide guidelines on subjects or actors of international law, it then describes all the relevant actors who participate in the digital information ecosystem and identifies their different capacities (section 2.2). The Chapter then suggests how actors may be identified in terms of their functional roles, applying a concept used in software engineering called the ‘use case diagram' (which defines the interactions between an actor and a system in relation to achieving a goal). Section 2.3 identifies and examines the functions that support the operation of the digital information ecosystem, while Section 2.4 considers their impact on enjoyment of human rights. The final section of the Chapter (Section 2.5) proposes a new typology of actors that have emerged in the digital information ecosystem and examines the degree to which the actors in the digital information ecosystem have legitimacy.

Introduction

At one time or another, we have all found ourselves unable to access a website. Websites may be inaccessible for many reasons. Users may simply mistype the name of the website they want; the servers that host the website in question may malfunction; the website itself may be momentarily unavailable; or the domain name system (which manages websites and assigns their names and numeric addresses) may be unable to link the requested domain name to its numeric address or may need time to build the correspondence between the website and its numeric address. Alternatively, some websites may be filtered and placed on a 'blacklist' by Internet Service Providers; or particular users may be blocked from accessing certain websites, on the basis of their IP (internet protocol) address. For instance, websites that host copyrighted contents such as Hulu and Pandora are only available in the United States, and websites that contains Nazi memorabilia are not accessible to users whose IP addresses are located in certain European countries.[1] Specific users may also be blocked from using an online platform by their administrator; for instance, a Facebook user who failed to abide by Facebook's internal codes and guidelines may be banned from accessing an account on Facebook. This list is not exhaustive.

The digital information ecosystem that supports activities carried out in the digital environment is like an onion and the layered nature of its architecture does not provide clear answers to many questions that ordinary users have. Individuals frequently lack knowledge or feel confused, and most are unaware of activities at deeper layers of the Internet that govern the exercise of their rights online. For users to fully enjoy their rights in the digital sphere, they need to understand who facilitates or impedes the exercise of these rights.

This statement immediately raises questions. What are these entities? How can we identify them? What is their purpose and function? What do they contribute to the Internet and the digital ecosystem? How do they impact the enjoyment of rights online?

This Chapter addresses such questions. It starts by examining the subjects of international law in the historical context of the international legal system (section 2.1). Having noted that the international normative legal framework does not adequately provide guidelines on subjects or actors of international law, it then describes all the relevant actors who participate in the digital information ecosystem and identifies their different capacities (section 2.2). The Chapter then suggests how actors may be identified in terms of their functional roles, applying a concept used in

[1] *Yahoo! Inc., a Delaware Corporatiom v. La Ligue Contre Le Racisme et L'antisemitisme and L'union Des Etudiants Juifs De France, 433 Fed. Reporter 3d 1199* (United States Court of Appeals, Ninth Circuit), 12 January 2006 .

software engineering called the ‘use case diagram’ (which defines the interactions between an actor and a system in relation to achieving a goal). Section 2.3 identifies and examines the functions that support the operation of the digital information ecosystem, while Section 2.4 considers their impact on enjoyment of human rights. The final section of the Chapter (Section 2.5) proposes a new typology of actors that have emerged in the digital information ecosystem and examines the degree to which the actors in the digital information ecosystem have legitimacy.

Terminology used in this report

This report is the second chapter of a thesis titled ‘Human Rights Obligations in the Digital Information Lifecycle and its Ecosystem’. Chapter One introduced the concepts ‘digital information’ and ‘digital information ecosystem’. To help the reader, this report includes a short explanation of these concepts, since they are referred to throughout the current report.

1. What is ‘digital information’?

Due to the advent of information and communication technologies, the digital sphere provides a range of communication tools, enabling individuals to express oneself and to communicate with one another in numerous ways: digital correspondence, digital chatting, instant messaging, video conferencing, participation in social networks, etc. However they are experienced by the ordinary user (as text, video, audio or photo), all these forms of action are finally converted into bytes. For instance, videos convert images into binary digits (0 or 1 bits), which are transmitted through optic fibres and then reconverted into images at their destination. The generally understood definition of information in the digital sphere is ‘any form of information that can be converted into bytes and presented in a digital format’.

2. What is a ‘digital information ecosystem’?

Digital information (in the form of bytes) cannot be transmitted autonomously. To transmit bytes from one location to another, equipment, devices, infrastructure and people are required. Digital information comes to life in the presence of functioning devices and equipment, physical infrastructure, functioning networks, and protocols. In other words, the life cycle of digital information relies on a larger system of interconnected elements, all of which interact to enable the transmission of digital information. In the thesis, this system and its elements are called the ‘digital information ecosystem’.

The technological devices that transform information into bytes and then retransform bytes into forms readable by human beings have evolved: desktops were followed by PDAs (personal digital assistants), smart phones and then smart watches, for example. After information is transformed into bytes, it is transmitted by electronic or other forms of signal, for example via copper wire, coaxial cable, optical fibre, satellite, or via airwaves at different bandwidths (channels). The points at which channels connect compose a 'network', which physically requires 'hardware' (such as routers, cables, switches and LAN cards) and 'software'. The interconnected network of all these physical elements is commonly known as the Internet. Digital information transmitted through a network uses an agreed language or 'protocol': when human users interact with hardware equipment, they use this computer language, also referred to as 'code'.

The concept of the 'digital information ecosystem' should be distinguished clearly from the terms 'Internet', 'cyberspace' or 'online space'. The Internet is the best known network for digital information transmission, but it is only one of many. Networks include closed intranet systems that are confined to a geographical space (Intranet) and systems that are not linked to public networks, such as local area networks (LANs) or the 'Darknet'. Whereas 'cyberspace' and 'online space' refer to non-physical domains, the digital ecosystem has a broader reference, not only to non-physical domains and the world of bytes but to physical equipment (in the form of atoms). 'Cyberspace' also has a distinctively social dimension in that it is not only a network of networks but a community of communities, where human beings meet, talk, buy and sell.

Body of Report

1. Actors in the international legal system

What human rights actors operate in the digital information ecosystem? Chapter 1 of this Study described the digital information ecosystem and its impacts on the international legal system. In this Chapter, we discuss the concept of 'human rights actor', as it developed in the international legal system of which the international human rights system is a part.

The discussion of actors is relatively new in international law and is seen to derive from political science. Traditional international law textbooks would not generally include a section on 'actors in international law' but would almost always write about 'subjects of international law' or 'international legal personality'. Recently, nonetheless, 'actors in international law' has become an important topic: it "touches on the very foundations of international law" and "determines who are the subject of the law in the international legal arena, who is entitled to make law, and who are regarded as the legitimate participants in the game".[2]

In any level of law, international or national, a legal person (or the subject of law) has the capacity to enter into legal relations and enjoys legal rights and duties in that legal system. This is referred to as having legal personality. The traditional indicators of legal personality in international law include having the capacity to make claims following breaches of international law, having the capacity to conclude international treaties and agreement, and the enjoyment of privileges and immunities from national jurisdictions.[3] Klabbers compares the notion of legal personality under domestic and international law in terms of the authority that confers or recognizes legal personality. Under domestic law, entities can possess a legal personality if they meet the requirements of that legal system; under international law, subjectivity and personality are conferred by an international legal system, which is composed of the academic community.[4]

The issue of subjectivity and legal personality in international law is the subject of ongoing discussion, reflecting the nature of international law which is considered part of the weave of social, political and economic relations, subject to constant change and development.[5] It is closely tied to the scope and definition of international law. As a result, the notions of legal personality and subject of international law have their roots in the history of international law, which merits a brief examination.

In the international legal system, the dominant view has been State-centric, which sees international law as a State-based system. In the nineteenth century, the subject of international law was understood to be solely and exclusively States and that international law only applied to States.[6] According to this traditional view, international law is founded on the common consent of individual States, which is evidenced by sources of international law including treaties negotiated by States and customary law, which is based on State practice and *opinio juris*.[7] Accordingly, international law is

[2] Andrea Bianchi, 'The Fight for Inclusion: Non-State Actors and International Law' in Rudolf Geiger Ulrich Fastenrath, Daniel-Erasmus Khan, Andreas Paulus, Sabine von Schorlemer, and Christoph Vedder (ed), *From Bilateralism to Community InterestEssays in Honour of Bruno Simma: Essays in Honour of Bruno Simma* (Oxford University Press 2011), 40.

[3] James Crawford, *Brownlie's Principles of Public International Law (*Oxford University Press, 2012), 115.

[4] Jan Klabbers, *An Introduction to International Institutional Law* (Cambridge University Press, 2009), 39.

[5] Robert McCorquodale, *International Law Beyond the State: Essays on Sovereignty, Non-State Actors and Human Rights (*CMP Publishing, 2011), 2.

[6] This originates back to 1648 Peace of Westphalia, which designated the State to be the primary source of power in international politics and law.

[7] Article 38 of the Statute of the International Court of Justice.

said to be rules which States have agreed through treaties, customs and other forms of consent; only States may participate in creating and enforcing international law.

This traditional view perhaps corresponded to social practice before the twenty-first century and the advent of the Internet. However, the modern world has substantially changed the environment in which traditional international law was developed. Several new phenomena help to explain why States have gradually delegated or relinquished some of their functions to private actors.[8] Among those, most relevant to the digital sphere are globalization and de-regulation. As noted in Chapter 1, for instance, the privatization of public utilities such as telecommunications has contributed to the rise of business entities in the telecommunication industry that have become very powerful actors in the digital information ecosystem.

This context, coupled with the need to protect individual rights from threats posed by non-State actors, challenged the dominant traditional view. While international law, according to the traditional view, is made by States to regulate inter-State activities and behaviour, the purpose of international human rights law is to protect individual rights whether these are threatened by States or non-State actors. The traditional State-dominant approach to human rights inevitably leads to the situation in which non-State actors whose conduct harms the enjoyment of human rights cannot be held legally accountable because they are not subject to direct legal obligations under international human rights law for violations of human rights they commit.

On these grounds, the notion that States are the only subject of international law has therefore increasingly been challenged and it is no longer accepted that States are exclusive actors in the international legal system. According to Andrew Clapham:

> “the burden would now seem to be on those who claim that states are the sole bearers of human rights obligations under international law to explain away the obvious emergence onto the international scene of a variety of actors with sufficient international personality to be the bearers of rights and duties under international law”.[9]

[8] Andrew Clapham, *Human Rights Obligations of Non-State Actors (Collected Courses of the Academy of European Law)* (Oxford University Press, 2006), 3-19. Clapham identified four important phenomena: globalization of the world economy, privatization, the fragmentation of States and an increase in internal armed conflict situations, and the feminization of human rights. See also Daniel Thürer, ‘The Emergence of Non-Governmental Organizations and Transnational Enterprises in International Law and the Changing Role of the State’ in Nils Geissler Rainer Hofmann (ed), *Non-state actors as new subjects of international law* (Ducker & Humbolt 1999), 39-40.

[9] Ibid, Andrew Clapham, 82.

Recent international law discussions have therefore begun to consider actors other than States, as well as the legal grounds on which they may acquire legal personality under international law. The *Reparations for Injuries* Opinion of the International Court of Justice opened this discussion when it alluded to the acceptance of non-State entities in the international legal system:

> "Throughout its history, the development of international law has been influenced by the *requirements of international life*, and the progressive increase in the collective activities of States *has already given rise to instances of action upon the international plane by certain entities which are not States*" [emphasis added].[10]

The ICJ Advisory Opinion clarified that subjects do not all possess the same rights and duties and that new actors may acquire legal responsibilities according to the needs of the community and the requirements of international life.[11] The 'needs of the community' calls for the international legal system to accept the broadened scope of its subjects. The way in which international organizations have obtained limited international legal personality indicates how relationships between *de facto* actors in society have changed. To perform their functions, international organizations needed to acquire an international personality, particularly the right to bring international claims. In the *Reparations Opinion*, the ICJ concluded that the United Nations is an international person "capable of possessing international rights and duties, and that it has capacity to maintain its rights by bringing international claims".[12] It is on this basis that international organizations have been granted a limited international legal personality.

To understand what the ICJ meant by 'needs of the community', an analogy can be made between chess and the international legal system. On a chessboard, the king is key to winning the game, but the pawns play an essential role in victory or defeat. As the game evolves, the initial purpose and status of the pawn can also change. If a pawn is advanced to its eighth rank, it may even be converted into a queen, rook, bishop, or knight. Similarly, it is the dynamic nature of the international legal system that will choose which actors may be converted and become subjects of the international legal system. In the context of the digital information ecosystem, the rise of digital technology has had a pervasive influence on daily life and has changed to the paradigm of the society, implying changes to the international legal system. Significantly, States and State entities played a comparatively small role in these changes. Most digital innovation and development was inspired by individual hobbyists and subsequently devolved to the commercial businesses as well as

[10] *Reparation for injuries suffered in the service of the Nations, Advisory Opinion, [1949] ICJ Rep 174*, 178.

[11] Ibid, 178.

[12] Ibid, 179.

to the users of their products and services. The history of the digital world suggests that its social norms were generated by technical community composed of individual experts. Later sections of this Chapter will describe how technical standardization entities and business manufacturers emerged to meet the needs of the international community in a digital information society.

In furtherance of and to complement the 'needs of the community' requirement, several theoretical approaches have been suggested as theoretical basis to confer status of subject of international law to non-State actors. Some of the suggested approaches include the concepts of participants in international legal decision-making process,[13] capacities in exercising specific rights and duties,[14] and 'international legal relationships'.[15] The number of such approaches indicates that no single normative approach has been agreed for that recognizes non-State actors as subjects of international law.

Furthermore, the approach of assessing whether an entity has become a 'subject' with 'status' under international law are subjective and are considered unhelpful. This is particularly true when the concept of participation in international legal process is applied to ascertain subjects in the context of the digital information ecosystem. International law is perceived to emerge from an established law-making process and scholars have proposed to identify actors of international law according to their participation in the legal decision-making processes, including the creation, development and enforcement of international law.[16] The capacity of actors to participate in international law-making and to enforce rules of international law is considered an essential aspect of conferring international legal personality.

However, participation in international legal processes cannot be assessed without defining the scope of international law. There is no definition of international law in terms of substance, apart from the assumptions that international laws are agreements concluded by heads of States through international organizations and that certain informal laws concluded by non-States (public authorities or individuals) may be elevated to the status of an international instrument with State consent. The concept of participation reverts to the State-centric approach of international law and become prone to circular reasoning.

[13] Rosalyn Higgins, *Problem and Process: Internatioanl Law and How We Use It* (Clarendon Press, 1994), 49. See also Robert McCorquodale, 'The Individual and the International Legal System' in *International Law Beyond the State: Essays on Sovereignty, Non-State Actors and Human Rights* (CMP Publishing 2011).

[14] Peter Malanczuk, *Akehurst's Modern Introduction to International Law (*Psychology Press, 1997), 93.

[15] C. Walter, 'Subject of International Law' in R. Wolfrum (ed), Max Planck Encyclopedia of Public International Law.

[16] Andrea Bianchi (ed), *Non-State Actors and International Law* (Ashgate 2009).

Some alternative approaches have been proposed to avoid this trap. Anthony Clark Arend has suggested that there are multiple levels of customary international law, some of which could be binding on all types of international actors. "The mutual interactions of a variety of international actors – states, substate actors, 'peoples,' and international organizations – would constitute general customary international law."[17] However, the proposal to establish customary international law building on interaction of wider range of actors would apply a subjective standard and it would be hard to fulfil the *opinion juris* element of customary international law. Most important, where the actors in a digital ecosystem are confined to that ecosystem, it would be difficult to argue that the interactions between them in that ecosystem constitute customary international law.

A point to retain from the theoretical discussion is that an inductive approach based on formalities should be avoided. Kate Parlett suggests that the key to determining whether actors are subject of international law is their actual ability to engage in international legal system in a given texts, not their formal status.[18] Similarly, Klabbers suggests that "personality is by no means a threshold which must be crossed before an entity can participate in international legal relations; instead, once an entity does participate, it may be usefully described as having a degree of international legal personality."[19] Furthermore, Andrew Clapham argues:

> "I recognize the importance of non-state actors and their influence without suggesting that they have achieved the role of law-maker. *We should indeed examine their activity and their interaction with states and others* to determine the duties and rights that states have fixed them with. Such an examination elevates them to subjects of interest without any automatic legitimizing effect [emphasis added]."[20]

These opponents of formal status as a criterion advocate for closing the gap between theory and practice; they argue that the behaviour of non-state actors in practice should determine their status in international law. For this to be reflected in the analysis on human rights actors in the digital information ecosystem, we need to develop a broader understanding of which actors have the capacity, and which actors actually participate in the digital information ecosystem. To do this, we first describe all the different actors in the digital information ecosystem and then analyse their

[17] Anthony Clark Arend, *Legal Rules and International Society* (Oxford University Press, 1999), 176.

[18] Kate Parlett, *The Individual in the International Legal System: Continuity and Change in International Law* (Cambridge University Press, 2011).

[19] Jan Klabbers, 52.

[20] Andrew Clapham, 28.

specific functions and the extent to which these functions qualify them to engage or participate in the international human rights system.

2. Actors in the digital information ecosystem

In this section, we consider a range of actors who participate in the digital information ecosystem and their capacities. A descriptive approach ultimately results in proliferation of non-State actors. It is nevertheless helpful at this stage to capture empirically the full spectrum of participants in the digital information ecosystem, looking particularly at how the ecosystem operates in practice. We look first at how actors in the ecosystem have been identified in existing literature and studies, then, based on these studies, suggest how the actors could be identified according to their functions.

2.1. Diversity of actors in digital information ecosystem

Human rights issues associated with the Internet and online environment, particularly the intersection of human rights and information technology, are addressed depending on the lens through which different disciplines look at the issue. Many studies have focused on certain rights or technologies, limiting their scope and resulting in a narrow coverage of related issues. Similarly, efforts to identify actors in the digital sphere have rarely taken a holistic perspective. To understand and address this deficit, we discuss below a few studies that have identified actors in the digital space.

Some studies focus on content regulation and freedom of expression. Seeking to apply freedom of expression principles to the Internet, Cucereanu identified the following actors involved in online communication: (a) Internet access providers; (b) host providers; (c) content providers (who 'fill' the internet with information and ideas); and (d) service providers, who enable authors and audiences to exchange opinions.[21] With the advent of content hosting platforms such as social media, blogging and search engines, a comparable study in 2013 identified a similar range of actors: its list included Internet service providers, web hosting providers, social media platforms and search engines.[22] Adopting a broader approach, a third study of freedom of expression online included several additional actors, such as data processers, web host providers, cloud computing services, domain names registries, and online media.[23] These examples suggest that, even in the context of one

[21] Dragos Cucereanu, *Aspects of Regulating Freedom of Expression on the Internet* (Intersentia 2008), 151.

[22] Article 19, *Internet intermediaries: Dilemma of Liability* (2013), 6.

[23] Rebecca Mackonnon and others, *Fostering Freedom Online: The Role of Internet Intermediaries* (UNESCO Publishing, 2014), 29.

specific right, categorizing actors is a subjective exercise influenced by the depth and the approach of each study as well as technological developments.

The above studies intentionally excluded technical aspects of the digital ecosystem, on the grounds that the technical structural administration of the Internet and associated technologies are "not the subject of regulation in respect of individual messages".[24] They focus on the regulation of harmful online content and protection of freedom of expression. Several civil society organizations promoted a similar advocacy line during the first World Summit on Internet Society (WSIS) in 2005. When WSIS included the topic of email spam on its agenda, it was accused of expanding its mandate and moving away from technical regulation into content regulation.[25] Similarly, in 2012, when the International Telecommunications Union (ITU) amended the International Telecommunication Regulations, Article 19 (an NGO that promotes freedom of expression) recommended that content regulation should not be part of the WSIS agenda because this would give ITU more control over content-related aspects of Internet policy.[26] Article 19 recommended that references to 'spam', 'cyber-crime', 'cyber-security', 'data preservation, retention, protection', 'protection of personal information, privacy and data', 'information and network security', 'fraud' and associated issues should be rejected.

This advocacy resulted in an artificial demarcation between content regulation and technical regulation and ignited technical-versus-policy discussions in the Internet governance area. The WSIS Declaration of Principles clearly states that "policy authority for Internet-related public policy issues is the sovereign right of States", limiting the role of the private sector and civil society to technical matters.[27] As the digital space has organically evolved, such an arbitrary designation of roles has

[24] Dragos Cucereanu, 146 (footnote 10).

[25] Ian Brown and Christopher T. Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013).

[26] Article 19, 'ITU: Draft of the Future International Telecommunication Regulation' (19 October 2012).

[27] First Phase of the WSIS (10-12 December 2003, Geneva), Declaration of Principles: Building the Information Society: a global challenge in the new Millennium WSIS-03/GENEVA/DOC/0004, para. 49; also Report of the Working Group on Internet Governance (June 2005), 8-10. More specifically, the report identifies the roles and responsibilities of government, the private sector and civil society. The roles and responsibilities of governments include: public policymaking, and its development, coordination and implementation; the creation of an enabling environment for information and communication technology (ICT) development; oversight functions; development and adoption of laws, regulations and standards; treaty-making; promotion of access to ICT services; promotion of the development of infrastructure and ICT applications; addressing general developmental issues; promoting multilingualism and cultural diversity; and dispute resolution and arbitration. The roles and responsibilities of the private sector include: industry self-regulation; development of best practice; development of policy proposals, guidelines and tools for policymakers and other

ceased to reflect reality. Indeed, it highlights a general failure to perceive the Internet and information communication technology as part of an interlinked ecosystem. By refusing to venture into the technicalities of the digital system, such an approach leads to examining the Internet as a forum that is only relevant to one's area of expertise and excludes many actors who play a role in the Internet and the digital ecosystem as a whole.

Additionally, as a result of evading the details on technical elements, commentators often fall into the trap of confusing the titles given to actors and their roles they actually carry out. They do so because academic literature and policy documents have not kept up-to-date with changes in the digital ecosystem, and the fact that many providers have taken on new roles. For instance, commentators use the terms 'Internet access provider' and 'Internet service provider' interchangeably to refer to entities that provide *access* to the Internet and entities that provide *services* on the Internet (such as hosting services). They also confuse the role of 'Internet service providers' and 'Internet content providers'. Broadly speaking, 'Internet service providers' provide infrastructure and services, which enable users to send data from one point to another. By contrast, 'Internet content providers' and 'Online service providers' distribute, manage and store information, among other services. At the beginning of the Internet era, business entities like America Online (AOL) acted as both the Internet service provider and the online service provider; they provided and controlled both access to the Internet and access to its content. Such institutions are referred to as 'walled-gardens', because they created borders within the Internet by selecting and providing content and information for users to access. The role of walled gardens changed when connection to the Internet no longer relied on dialup connections. Today, broadband connection services allow users to connect directly to the Internet without a middleman.[28]

Other studies have rightly pointed out that the new information technology involves not only users and providers of information but also designers of the technology and service providers.[29] The current Special Rapporteur on Freedom of Expression, David Kaye, has categorized the technical

stakeholders; research and development of technologies, standards and processes; contributing to the drafting of national laws; participation in national and international policy development; fostering innovation; arbitration and dispute resolution; and promoting capacity-building. The roles and responsibilities of civil society include: awareness-raising and capacity-building; promotion of various public interest objectives; facilitating network-building; mobilizing citizens in democratic processes; bringing in the perspectives of marginalized groups, including, for example, excluded communities and grass-roots activists; engagement in policy processes.

[28] Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Vintage, 2011), 262 – 263.

[29] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (E/CN.4/1998/40), para. 30.

actors involved in design of the technology, and also identified private actors and their roles in organizing, accessing, populating and regulating the Internet.[30] Nevertheless, the focus on one specific right – even though it promotes in-depth analysis – tends to marginalize certain actors and relevant concerns. For instance, the Special Rapporteur's list omits some actors that facilitate communication or transactions on the Internet. These play important roles. Certification providers, for instance, authenticate digital identity by issuing digital certificates that are also used for secure communication. Financial intermediaries accommodate online transactions (such as credit card purchases). The mode of payment and the personal identification information that are associated with the user (such as credit card owner)are often used as a means to identify users. Similarly, online advertisement is the primary business model of all Internet services, but this too is not addressed. At first sight, the core roles of these actors do not directly affect freedom of expression. Indirectly, their influence is critical, however, because they have the power and the capacity to authenticate or reveal the identity of users and have control over personal data that flows within the digital space. The importance of these factors is evident in electronic commerce, which has developed a range of regulatory and authentication tools to facilitate commercial transactions and build legal certainty for businesses and consumers.[31]

When the focus shifts from a specific right to a specific technology, it becomes clear that many technical elements were not visible in past research. Research that focused on surveillance technologies identified the following business actors in the ICT sector: device manufacturers that manufacture or sell mobile devices, computers and digital cameras; network equipment manufacturers that produce semiconductors, switchers and routers; network management providers that provide telecommunication, wireless and Internet services; and connectivity/access management providers that provide web-based services and platforms such as search engines, social

[30] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (A/HRC/32/38) (2016), paras. 15 – 25. He distinguishes nine kinds of actor, who (1) enable connection to the Internet, such as Internet service providers and telecommunication service providers; (2) design and maintain hardware and operating systems that facilitate information processing and Internet access, such as infrastructure vendors and equipment manufacturers; (3) allocate web domains; (4) host information, such as web-hosting service; (5) facilitate aggregating, sharing and searching information (search engines); (6) produce and regulate access to content; (7) connect users and communicate; (8) sell goods and services and facilitate transactions; and (9) collect, repurpose and sell data.

[31] Note by the Secretariat, 'Present and possible future work on electronic commerce', submitted to the forty-fourth session of the United Nations Commission on International Trade Law (A/CN.9/728).

networking, emails and cloud computing.[32] Research that focuses on the potential of video usage with respect to human rights identifies actors who help users to employ technology safely and effectively: technology companies and developers; technology investors; human rights and civil society organizations; funders; and policy-makers and lawmakers.[33] If the focus is on manufacturing, the business actors in the ICT ecosystem extends from telecom equipment manufacturers (who provide fixed and wireless telecoms network equipment) to content providers.[34]

In sum, an analysis of the literature on actors in the digital space suggests that actors perform several roles, which change under the influence of other actors and a range of other variables. It is therefore not only impossible but also ineffective to categorize actors in the digital space on the basis of one right, one technology, one standard or one perspective alone. Acknowledging this, at international level some recent initiatives have taken a more inclusive approach and recognized multi-stakeholders as actors. The most notable example is the WSIS, which noted already in 2003 that management of the Internet involves both technical and public policy issues and should involve all stakeholders, including States, the private sector, civil society organizations, intergovernmental organizations and international organizations.[35] In the human rights area, the African Declaration on Internet Rights and Freedom (adopted in August 2014) recommended prescribing specific roles to regional and sub-regional bodies, national governments, international organizations, civil society organizations, media institutions, companies, technical communities, and academic, research and training institutions.

Including all stakeholders makes it possible to analyse all the actors in the digital information ecosystem. However, considering that the digital information ecosystem touches almost every discipline, identifying all stakeholders and actors will generate an endless list. To overcome this

[32] International Federation for Human Rights (FIDH), *Surveillance Technologies 'Made in Europe': Regulation needed to prevent human rights violations* (2014), 7.

[33] Witness, *Cameras Everywhere: Current challenges and opportunities at the intersection of human rights, video and technology* (2011), 30-35.

[34] More specifically, actors include: providers of software, such as routers and radio base stations; providers of consumer electronic devices (manufacture of cell phones and other mobile devices); providers of telecommunications services (local and international telecommunications services); over the top companies, who deliver internet services, develop enterprise services and security software, and deliver content; and third party companies that offer applications for download by consumers in areas such as entertainment, business, health or education. See Ericsson, *ICT and Human Rights: An ecosystem approach* (2013), 9.

[35] First Phase of the WSIS (10-12 December 2003, Geneva), Declaration of Principles: Building the Information Society: a global challenge in the new Millennium WSIS-03/GENEVA/DOC/0004.

problem, in the next section I propose a method for identifying actors based on their functional roles, which constitute critical components of the digital information ecosystem.

2.2. Proposal: identifying actors based on their functions

The diversity of actors in the digital information ecosystem and how international human rights law considers actors requires us to take a step back. What is the basic definition of 'actor'? According to Black's Law Dictionary, an actor is 'one who acts' and 'a person whose conduct is in question'. Building on this definition, the question we need to ask is: who acts in the digital ecosystem? To answer this, I propose adopting the 'use case' concept employed in software engineering.[36]

Like the scenario of a movie, a 'use case' is a list of actions or steps taken to achieve certain goals. This step-by-step approach generates a 'use case' diagram that describes the interactions between an actor and the system. An 'actor' may be a person, a company or organization, a computer program, or a computer system (hardware, software, or both). The diagram also defines stakeholders, who do not necessarily interact in the system or with other actors but have an interest or are entitled to know how the system is working. For example, stakeholders might include regulatory bodies or a company's board of directors. The diagram also shows, in simplified, graphical form, what the system must do to accommodate the goals in question. More specifically, it illustrates the system's behaviour, highlighting what must happen in the system (including its software systems and other elements) to achieve the goals.

The digital ecosystem is a combination of 'use cases', and has many components that interlink in complex ways. Taken as a whole, the components support the activities and actions that individuals take in the digital space. A number of actors are responsible for each component and are tasked with functions associated with them. Put simply, a range of actors perform a range of functions that constitute fundamental components of the digital information ecosystem and are essential to the operation of the ecosystem.

Behind a computer screen and a mouse, it is said that 'nobody knows you are a dog'. On the Internet, the identity of the user and the status of the user are not easy to determine. It follows that the status of users should not be the starting point for analysing the system's actors. It is better to focus instead on their functions in the digital ecosystem. My proposal is to shift the focus and look at 'what' rather than 'who'. Examining what relevant actors do will cause us to concentrate on violations (rather than violators) and on the protection of individuals whose rights are violated.

[36] The use case model is also used in Chapter 3 to identify the specific responsibilities of human rights actors in the digital ecosystem.

Freedom in the digital ecosystem depends on the choices and actions that all actors take; and actions should be taken and judged on the basis of a well-founded understanding of who does what, where.

A function-based approach has several advantages. First, if we address what actors actually do, it will become easier to establish what they ought to do. The roles of actors in the digital ecosystem are often unclear, as are their relationships. As a result, it is difficult to understand how power and control are exercised and to establish adequate measures of accountability. Clarifying actors' roles will also help to make clear their human rights obligations in the digital information ecosystem. If we want to ensure that all actors in the digital space abide by their human rights obligations and responsibilities, and want to monitor this properly, we need to understand exactly who the actors are, and what they do, in practice. As Jan Klabbers notes, before assigning responsibility to entities, it is important to establish that they "actually had something to do with the matter and that it is reasonably clear what part of their actions was theirs".[37]

Second, a function-based approach can resolve the long debate about the separation of policy and technical issues. The separation of entities that perform technical functions (limiting their role to the technical realm) from entities that regulate content on the Internet has been a constant source of contention, particularly in the area of Internet governance. The analysis below of functional components of the digital information ecosystem demonstrates that the private sector can equally implement public policy and can fulfil decision-making functions by programing 'codes' or internal codes of conduct.

Third, as actors and their roles change over time, it is necessary to assess their specific roles in order to prevent human rights harms and redesign human rights monitoring to meet the needs of evolving roles of actors in the digital information ecosystem. The pace of change in Internet services, and their technical complexity mean that it is difficult to establish stable and consistent business practices. This is clear from the business models of online service providers: companies whose initial business model was based on providing products or software (such as online platforms or word processing software) now provide infrastructure, a new business model. Facebook, for instance, a social network platform, now provides Internet connection services through an Internet-delivery drone.[38] Instead of identifying and categorizing business entities in terms of specific roles, my suggestion is therefore to identify and categorize actors according to the functions they fulfil in the

[37] Jan Klabbers, 274.

[38] Jessi Hempel, 'Inside Facebook's Ambitious Plan to Connect the Whole World', WIRED (January 2016). At: https://www.wired.com/2016/01/facebook-zuckerberg-internet-org/.

digital information ecosystem. This approach has the further advantage that categories are less likely to become obsolete due to the rapid development of information technology.

3. Functions constituting core elements of the digital information ecosystem

Having established the advantages of a function-based approach, the next step is to describe key functions. The next section could be said to fall outside the discipline of international law. However, legal scholars too often underestimate or ignore the role and importance of the technical dimensions of the digital information ecosystem, diminishing understanding and making misguided assumptions. Some even simply exclude technical aspects of Internet governance from discussion, claiming they do not belong in the public policy realm. Yet, in several instances technologies and technical entities have played an essential part in protecting human rights (for instance, through using encryption) or violating them (for instance, using filtering technologies). To understand the technical dimensions of the digital information ecosystem, it is indispensable to examine whether particular functions or activities promote or violate rights online. Without such an examination, mere theoretical discussion of actors and roles will be inadequate to address the complex architecture of the digital information ecosystem.

At the outset, it should be emphasized that the digital information ecosystem is like a living document subject to change as technology and components of the ecosystem evolve. The digital information ecosystem of the 1990's relied on dial-up connection, so telephone companies were major player and desktop computers were the device of choice. In the second decade of the twenty-first century, connections are made using wireless networks and hand-held mobile devices dominate. Both the technology (desktop computer versus mobile device) and the actors that implement the functions (telephone companies versus wireless network providers) changed – and will change again. Yet the functions of ecosystem will continue to persist, because they are the core architecture underlying the digital information ecosystem.

It is important also to reaffirm the *capacity* of individuals in the digital information ecosystem. As introduced in Chapter 1, the 'openness' of the digital ecosystem enables individual users to do many things without the assistance of government or businesses. The actors in the digital ecosystem often fulfil roles that do not depend on State consent or the State's intervention or assistance. Individuals, business entities and government entities alike can be involved in operating critical functions of the digital information ecosystem.

The section below describes some of these critical functions, grouped under the following headings: provision of products and services (including devices, network, infrastructure, platform, software and certification); use of the system; allocation of resources; creation of technical standards; and creation of laws (including informal and formal law as well as private codes and procedures).

A number of relevant functions, for instance education and awareness-raising, are not included because they are secondary to the operation of the digital ecosystem. Functions that are part of the life cycle of digital information (its creation, transmission, collection, processing, storage, disposal) are also excluded at this stage because they are not functional components but operations undertaken at specific stages of the life cycle.[39]

3.1. Provision of products and services

Because they are a distinctive feature of the digital information ecosystem, third party providers and their roles were emphasized in Chapter 1. In this section, we examine in more detail both the types of third party providers that exist in today's digital information ecosystem structure and their functions. The ability of users to carry out activities in the digital sphere depends on these functions (provision of products and services).

In the online world, third party providers are generally assumed to be business entities. They are usually referred to as 'providers' or 'online/internet intermediaries' who provide products or services that facilitate and are part of the digital information ecosystem.[40] However, as noted earlier, while business entities are providers, they are not the only providers within the system.

We have classified providers in terms of the component they contribute to the digital information ecosystem: devices and software, network connectivity, web-based services, or certification.

3.1.1. Devices and software

Some manufacturers of equipment and devices produce electronic consumer devices such as computers and hand-held devices that are used to convert information into digital format or to connect to the network. Others produce devices such as routers and servers, which are the physical instruments on which the digital ecosystem relies. Still others provide applications or software that

[39] The life cycle of digital information is reviewed in Chapter 3, which argues that it offers a framework for assessing specific responsibilities and obligations of human rights actors in the digital information ecosystem.

[40] OECD describes Internet intermediaries as entities that "give access to, host, transit and index content originated by third parties or provide Internet-based service to third parties". It suggests that the main functions of Internet intermediaries are to: (i) provide infrastructure; (ii) collect, organize and evaluate dispersed information; (iii) facilitate social communication and information exchange; (iv) aggregate supply and demand; (v) facilitate market processes; (vi) provide trust; and (vii) take into account the needs of both buyers and sellers. Organisation for Economic Cooperation and Development, *The Economic And Social Role Of Internet Intermediaries* (OECD Publishing, March 2010).

run on equipment and devices. Some entities (such as Apple) provide both devices and downloadable software that runs on them, including the operating system and web browser. Others (like the EndNote citation management system) provide standalone software, which consumers pay a subscription or licence fee to access.

While many devices and software are commercial products provided by business entities, individuals and government bodies also have the capacity to equally create, supply and distribute devices and services. The influential role of individuals in the computer industry has been highlighted since the 1980s.[41] Apple, a technology company that sells electronic consumer products, was started by two individuals, Steve Wozniak and Steve Jobs, who created the first personal computer (called 'the Apple') in Steve Jobs' home. Microsoft, a technology company that is best known for selling computer software, was also started by two individuals, Paul Allen and Bill Gates.

3.1.2. Network connectivity

Second, entities provide the means to connect to networks, both local networks confined to a specific place and open networks like the Internet. The constitution of the International Telecommunication Union uses the term 'operating agency' to refer to individuals, companies, corporations or government agencies that operate telecommunications installations intended for an international telecommunication service. We will use the term 'network service provider' to refer to entities that provides user connectivity to the Internet.

As the definition suggests, several types of entity can act as network service providers. Before privatization, most telecommunication companies began as State-owned companies. In some countries, the government still manages network service providers or controls the number of fibre-optic links in and out of the country. In addition to businesses and governments, international organizations, such as international satellite organizations, provide network infrastructure using satellites.[42]

3.1.3. Web-based services: infrastructure, platform and application

Some entities provide web-based services or services based on cloud computing technologies. In general, "cloud computing technology refers to the delivery of information technology resources as

[41] Walter Isaacson, *The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution (*Simon & Schuster, 2015).

[42] Patricia K. McCormick, *Neo-Liberalism: A Contextual Framework for Assessing the Privatisation of Intergovernmental Satellite Organisations* (Martinus Nijhoff Publishers 2014).

a service to multiple customers through the Internet: a process whereby software, shared resources and information are held on remote servers designed and established by the respective network or infrastructure operator”.[43] These differ from conventional applications which are downloaded and installed on the local system of each user and remain under the user’s control. Cloud-based services are hosted and saved on the ‘cloud’ and service providers control the handling of data.

The nature of cloud computing can be made clear by comparing it to the management of service apartments.[44] In serviced apartments, the occupant focuses on managing his or her living space and enjoying its services; all other activities (such as maintaining the building and its services) are handled by a service provider. Similarly, users of the cloud enjoy access to electronic communications while relying on their provider to manage data storage and maintain the shared servers, data storage and other elements of the system that they share.

Services can be classified more concretely into: (a) basic computing in structures that deliver processing power or storage (“Infrastructure as a Service”); (b) platform and tools such as operating systems, database management, web servers (“Platform as a Service”); or (c) application software such as email management (“Software as a Service”).

Most consumers are familiar with the application services associated with software as a service: blogs, wikis and other text-based collaboration formats, instant messaging, photo sharing sites, social network sites, computer games, video content, file sharing sites, etc. These applications can be developed and operated by any actors in the digital information ecosystem: individuals can program and operate a simple website with self-operated servers; businesses can develop commercialized platforms for services like Twitter and Facebook; governments can build their own websites to provider e-government services to citizens; international organizations can run platforms, for example to provide information on customs fees and taxes for services and goods traded around the world (the International Trade Organization’s Trade Map);[45] while non-government and civil society organizations can also develop platforms, for example on resolutions adopted by the Human Rights Council (HRC resolution portal operated by the Universal Rights Group).

Individual customers are less familiar with Platform as a Service because these mainly target market players that use them to develop and host proprietary solutions or provide services to third

[43] Xiaoxi Fan and K.P. Chow Joe Kong, ‘Introduction to cloud computing and security issues’ in Anne S.Y. Cheung and Rolf H. Weber (ed), *Privacy and Legal Issues in Cloud Computing* (Edward Egar Publishing 2015), at 8.

[44] This analogy is borrowed from ibid , at 13.

[45] Website at: http://www.trademap.org/Index.aspx

parties. Operating systems, database management, security and workflow management, and web servers are provided so that users can construct, install and develop their own applications. Providers of platforms merely enable users to create content and share information and do not enjoy editorial control over their content. Because these platforms do not themselves create or own the content that is published or broadcast on them, but facilitate social communication and information exchange, Platforms as a Service are sometimes called 'participative networking platforms'.[46]

Lastly, providers of Infrastructure as a Service provide virtualized computing resources and computing infrastructure over the Internet. For instance, they host Internet servers and domain names; in other words, they rent web server space that permits clients to set up their own websites.

3.1.4. Certification

The digital sphere lacks the certainties that exist in person-to-person relationship and transactions. To overcome this, and provide a more secure environment for transactions and other activities, several methods have been developed for accrediting and certifying digital transactions and the identities of those who engage in them.

A prominent example is the use of 'digital certificates', often used interchangeably with 'public key infrastructure' (PKI). The concept of PKI refers to the technical components, policies and procedures required to create, distribute, store, revoke and manage a digital certificate that asserts the authenticity of a digital signature. Broadly speaking, the purpose of a digital certificate is to confirm the identity of users during an electronic transaction, and confirm the authenticity of documents or verify their content. To perform its function, a digital certificate must establish a link between the digital signature embedded in the digital certificate and the holder of that signature. This requires an additional mechanism where a trusted third party confirms that the signature matches the signatory by issuing a certificate.

As well as certificates that authenticate identities and information, there are other forms of certification. The online industry is largely premised on the convenience of payment via financial intermediaries such as credit card companies. While the primary function of financial intermediaries is to facilitate remote payment, in the process of doing this the intermediaries also authenticate users by providing personally identifiable information associated with their credit card and bank accounts.

[46] Organisation for Economic Cooperation and Development, 9.

A third type of certification upholds the quality and standard of products. The International Electrotechnical Commission manages Conformity Assessment Systems which certify that equipment, systems or components conform to international standards. Accredited certification bodies (national accreditation bodies or private entities) issue certifications in accordance with the ISO's Committee on Conformity Assessment certification process.

3.2. The function as user of the digital information ecosystem

Users of the Internet may be individuals, professional journalists using Internet as a media outlet, or representatives or automated computers of a government or any other organization. These entities may be clients enjoying the services offered, or may be products of the digital information ecosystem.

First, users as clients or consumers can be described in terms of how they use the digital information they obtain or generate. Passively, users use the Internet for non-expressive tasks such as online shopping, online financing, and other transactions; they enjoy the services and products provided by other actors. These users are not limited to individual users; governments and any organization can be 'clients' or 'users' when they use digital information and its ecosystem to communicate, offer services and applications, or develop content.

Actively, users use digital information to create new forms of art and expression, irrespective of whether the created outcome is copyright protected. These users are called 'prosumers' (a person who consumes and produces media). Users may also distribute or populate content that has been created by others. For instance, they may share, rate (evaluate), label, and review such content. Prosumers can be described according to their capacity to use technical elements of the digital ecosystem. The spectrum of expertise that users possess ranges from comprehensive knowledge on information gadgets and services to general knowledge based on frequent Internet use. Users may be individual amateurs or hobbyists or 'power users' who possess a technical capacity and expertise comparable to that of a business. They can create or contribute to the development of technical and content aspects of the digital ecosystem by designing and programing products and services that are used by others. The role of creator in the digital ecosystem is not limited to natural persons; government bodies and other legal entities can be creators.

Second, users who consume the products and services offered in the digital environment can also be products of those services. Information about users can itself be a product and, in this sense, even when passive, users are knowingly or unknowingly part of the ecosystem. Users can be customers and at the same time the product of data processing entities such as Google. When individual users use Google's search engine to find information on the Internet, Google uses search queries to obtain information about users. Social network sites have adopted a similar business model; they transform information about users into a commodity that they sell to advertisers. Tim Wu has called those who employ this business model to raise revenue 'the attention merchants' because it converts users' attention users into revenue, usually via advertisements.[47] Gradually, users of the digital ecosystem have come to accept this practice: in effect, in exchange for convenient access to service and products online, we allow nearly all parts of our lives to be commercially exploited and accept the presence of advertisements alongside all that we see.

3.3. Allocation of resources

Two forms of resource allocation can be considered: allocation of frequency and spectrum; and allocation of domain names and Internet Protocol (IP) addresses.

In relation to allocations of frequency and spectrum, the International Telecommunication Union allocates frequency bands to categories of communications services. These include the allocation of bands on the radio-frequency spectrum, the allocation of radio frequencies, the registration of radio-frequency assignments, and, for space services, the allocation of orbital positions for geostationary satellites and the allocation of other characteristics of satellites in varying orbits.[48]

Some entities manage resources associated with global naming and addressing capabilities. They allocate and assign unique identifiers (such as domain names and IP addresses) that direct the movement of data across the Internet. Essentially, they decide who has what number(s) and for how long.

Individual experts initially had control over the management of Internet domain names. At the start of the Internet era (from 1988 to 1998), the Internet domain name registry was managed by two individuals at the Information Sciences Institute of the University of Southern California.[49] Subsequently, its management was transferred to a private business entity, Network Solutions Inc. (NSI).[50] As administrator of the domain name registry, NSI enjoyed a monopoly and at one point charged USD100 to register a domain name. To end the monopoly and allow new private organizations to enter the market, the Internet Corporation for Assigned Names and Numbers (ICANN) was established to oversee the registration of domain names and their accreditation.

[47] Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads (*Alfred A.Knopf, 2016).

[48] Article 1(2)(a) of the Constitution of the International Telecommunication Union.

[49] Jon Postel and Joyce Reynolds, under a contract with the US Defense Advance Research Project Agency.

[50] NSI operated domain name registry services on behalf of the US Government.

ICANN is the technical coordinator of the Internet's Domain Name System and is responsible for coordinating the allocation and assignment of Internet Protocol (IP) addresses. ICANN also manages the Internet Assigned Numbers Authority (IANA), which in turn manages the root server and coordinates the allocation of IP addresses to five Regional Internet Registries. The Regional Registries are private and non-profit and manage IP addresses in a geographical region. They also allocate a block of IP addresses to Local Internet Registries, which can be Internet service providers, private companies or academic institutions. On 1 October 2016, the IANA contract between ICANN and the United States Department of Commerce National Telecommunications and Information Administration expired. Public Technical Identifiers, a new affiliate of ICANN, now provides IANA functions.

3.4. Creation of technical standards

From a technical perspective, activities in the digital information ecosystem are made possible by implementing technical standards. Many individual users unknowingly agree to use these standards. For instance, by typing 'https://' in their web browser, consumers are consenting to use the hypertext transfer protocol (HTTP). Technical standards have two elements. A set of processes determines how information is processed, managed and distributed; and technical specifications determine the standards to which a product is manufactured. The term 'technical standards' is used in lieu of the term 'private regulation' in order to connote its primary purpose of ensuring interoperability within the digital information ecosystem. Put more simply, technical standards are an implicit promise or agreement among users to use the same protocols, similar to the postal sector uses agreed post codes and the customs sector applies an agreed nomenclature for goods.

As described in Chapter 1, digital information travels through various layers of the digital ecosystem; each layer is associated with different technical standards, which as a whole constitute the backbone of the ecosystem.[51]

In the first layer, information converted into digital format is transmitted across a physical network, (namely, channels across which the digital information travels). Information can be transmitted in several ways and at different bandwidth according to the channel (copper wire, coaxial cables, optical fibre, satellite, or airwaves). The most widely known technologies are wireless

[51] The most detailed conceptual model that explains the different layers of the digital information ecosystem is the Open System Interconnection (OSI) model composed of physical layer, data link layer, network layer, transport layer, session layer, presentation layer and application layer.

networks, such as Wireless Local Area Network (WLAN), 3G or 4G, and WiMAX.[52] At this level, the physical network is regulated by international standards (such as security protocols developed by the technical community[53]) and national standards implemented in a specific country.

Depending on the type of network, different entities are involved in technological standard-setting processes: for example, the Groupe Spéciale Mobile Association (a private international association of the mobile industry) develops standards for mobile networks, while the Institute of Electrical and Electronic Engineers (IEEE) develops standards for Wi-Fi transmission. At global level, the International Telecommunication Union (ITU) is mandated to facilitate the worldwide standardization of telecommunications.[54] The ITU's Telecommunication Standardization Sector (ITU-T) coordinates standards for telecommunications and every four years, the World Telecommunication Standardization Assembly is convened to consider specific matters related to telecommunication standards.

To enable digital information to reach its intended recipient, it must be accompanied by information that indicates its destination. These unique identifiers direct the movement of data across the Internet, and include domain names and Internet Protocol (IP) addresses. IP addresses enable data to move from departure points to destination points within a network. At the second layer, digital information is broken into data packets, which contain information that enables the transmission of the data packets (datagrams) between hosts and across networks. This layer is concerned with IP addressing protocols, which specify the format of packets and the address scheme of the network.

[52] WLANs provide wireless network communication over short distances using high frequency radio or infrared signals instead of traditional network cabling. A WLAN typically extends an existing wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network. 3G is the third generation of mobile phone standards and technology based on the International Telecommunication Union (ITU) family of standards. 3G networks enable operators to offer wider range of services like video calls, voice telephony, and achieve great network capacity. WiMAX (Worldwide Interoperability for Microwave Access) is a wireless networking technology, which allows higher speeds and longer distances than classic Wi-Fi.

[53] Some examples of standards relevant to the physical network level are: Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2), which are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.

[54] Article 1(2)(c) of the Constitution of International Telecommunication Union. ITU's standardization process started with the Consultative Commission for both international telephone service and long distance telegraph in 1925, which were merged to International Telegraph and Telephone Consultative Commission (CCITT) in 1956. Subsequently, CCITT was changed to Telecommunication Standardization Sector (ITU-T) in 1992. Until 1989, telecommunications equipment standards were approved every four years as recommendations by the former CCITT.

The third layer transports the information (transport layer). Here, level of service and the status of connection used to transport data are defined. The relevant standards for this layer are: the transmission control protocol (TCP); and the user datagram protocol (UDP). TCP ensures that a data packet reaches its destination by checking on its arrival. The UDP protocol makes it possible to send data (such as music or movies) faster.

At the fourth layer (the application layer), standards and protocols facilitate the interchange of information from one computer to another. The protocols used include the file transfer protocol (FTP), the electronic message protocol (SMTP), and the hypertext transfer protocol (HTTP). Although it was not implemented, an effort was made to develop a platform for privacy preference (P3P) standards. This would have allowed web sites to describe their data collection and processing practices in machine-readable format.[55] In theory, it would allow users to configure their Web browser, permitting them to provide personal data only to sites whose privacy policies they accepted.

Lastly, the International Electrotechnical Commission (IEC) of the International Standard Organization (ISO) prepares and publishes standards for all electrical, electronic and related technologies. Its protocols apply to all layers. IEC International Standards cover a vast range of technologies, from power generation, transmission and distribution to home appliances and office equipment via semiconductors and fibre optics. The ISO establishes standards but is not involved in certification processes and does not issue certificates.

3.5. Creation of laws and non-laws

In the international legal system, laws are traditionally negotiated and drafted in a forum hosted by international organizations; heads of delegates with accredited authority formally negotiate and conclude a legally binding instrument. In fast-changing environments such as the digital sphere, swifter, less bureaucratic and more flexible ways to establish laws and regulations seem to be favoured. Because of the difficulty to conclude international agreements, and reach universal consensus, recently actors have increasingly opted for less formal preparatory phrase for concluding international agreements, for instance in the form of guidelines, declarations, principles or codes of conduct.

According to Pauwelyn, informal international law-making is characterized by output informality (it does not result in a formal treaty or traditional source of international law), process informality (it

[55] Members of the World Wide Web Consortium were unable to reach a consensus on the second version of the standard and its development was suspended in 2007.

takes place in a forum other than a traditional international organization), and actor informality (it involves actors other than traditional diplomats).[56] Pauwelyn's definition focuses on informal law-making by public authorities which are not traditional diplomatic actors and therefore lack accredited authority to represent and bind a State. These actors include ministry officials, domestic regulators, independent or semi-independent agencies, sub-federal entities, or members of the legislature or judiciary.[57] Essentially, it identifies regulatory and agency networks that do not issue legally-binding documents, but excludes forms of lawmaking that are initiated by purely private actors without the involvement of accredited authorities. We take a broader, more inclusive approach. On the presumption that private entities significantly influence the digital environment, we take account of private entities as well as public authorities when we consider informal law-making and the generation of 'non-laws', such as internal procedures and codes of conduct.

We distinguish four types of informal law-making mechanism, drawing on Benvenisti's classification as well as the mechanisms described below in this section: (1) informal inter-governmental agreements; (2) informal agreements by public and private institutions; (3) transnational private regulations; and (4) informal interpretations by private actors of formal positive international law.[58] In addition to these four types, we also examine the traditional inter-governmental law-making process.

3.5.1. Formal inter-governmental agreements and treaties

Though informal law-making has become dominant in the digital technology industry, traditional and formal law-making continues. As the digital information ecosystem cuts across a wide range of disciplines, related law is cut-across multiple aspects. This said, the number of legislation at international level are relatively little because the speed of technological change in the sector has outpaced the formation of international law.

At international level, most of the instruments negotiated and concluded by member States focus on trade and commercial aspects of digital technology. The World Intellectual Property Organization (WIPO) concluded two treaties ('the WIPO Internet treaties') in 1996 that updated copyright and related rights for digital media. Other international instruments include the World Trade

[56] Joost Pauwelyn, 'Informal International Lawmaking: Framing the Concept and Research Questions' in Ramses A. Wessel Joost Pauwelyn, and Jan Wouters (eds), *Informal International Lawmaking* (Oxford University Press 2012), 15-20.

[57] Ibid, 19.

[58] Eyal Benvenisti, 'Towards a Typology of Informal International Lawmaking Mechanisms and their Distinct Accountability Gap' in ibid .

Organization's Basic Telecommunication Service Agreements, UNCITRAL texts on electronic commerce and electronic signature, the ITU's International Telecommunication Regulation (amended in 2012). In 2013, countries participating in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies agreed to restrict the export of dual use ICT products, such as intrusion software and network surveillance systems.

At regional level, the European Union's data protection rule is the most prominent example of hard law on digital technologies. EU Data protection rules have been amended. The General Data Protection Regulation (GDPR) will enter into force in May 2018, replacing the Data Protection Directive of 1995.

3.5.2. Informal inter-governmental agreements

States have produced several soft inter-government agreements that were not negotiated by accredited delegations and are not legally binding. They nevertheless influence the behaviour of the parties concerned. As Benvenisti has pointed out, though informal rules are not binding on the parties that agree them, they informally modify the rights and obligations of other actors.[59]

Examples include: the United Nations Guidelines for Data Protection;[60] the United Nations Guidelines for Consumer Protection, agreed by the United Nations Conference on Trade and Development;[61] UNESCO's recommendation on the promotion and use of multilingualism and universal access to cyber space; and, most notably, the Guiding Principles on Business and Human Rights, which sets out the United Nations "Protect, Respect and Remedy" Framework.[62]

The Framework sets out: the duty of state to protect against human rights abuses by third parties, the responsibility of private companies to respect human rights, and the need to provide individuals and communities whose rights are infringed with access to effective judicial and non-judicial remedies. Initially, the Guiding Principles were the final product of the mandate of the United Nations Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie (presented to the United Nations Human Rights Council in 2008). However, exceptionally, the United Nations Human Rights

[59] Ibid , at 299.

[60] United Nations Guidelines for the Regulation of Computerized Personal Data Files (resolution 45/95) (14 December 1990).

[61] The guidelines were first adopted by the General Assembly in resolution 39/248 of 16 April 1985, later expanded by the Economic and Social Council in resolution E/1999/INF/2/Add.2 of 26 July 1999, and recently revised by the General Assembly in resolution 70/186 of 22 December 2015.

[62] See, A/HRC/17/4 and A/HRC/17/31.

Council composed of member States endorsed the Guiding Principles, elevating it to an authoritative reference for States, business and civil society organizations.[63] The Guiding Principle is now widely benchmarked. For instance, the European Union is preparing Guidance for the Information and Communication Technologies Sector on Implementing the UN Guiding Principles on Business and Human Rights.[64]

Intergovernmental coordination of policies provides a different example of informal intergovernmental agreement. The purpose of the World Summit on Information Society (WSIS) is to formulate a common vision and understanding of the global information society and to harness the potential of knowledge and technology to promote the development goals of the Millennium Declaration.[65] WSIS developed in two phases: the first in Geneva in 2003, and the second in Tunis in 2005. The objective of the Geneva phase was to develop and foster a clear statement of political will and take concrete steps to establish the foundations of an information society for all. The objective of the Tunis process was to put the Geneva 'Plan of Action' into effect and to find solutions for and reach agreements on Internet governance.

3.5.3. Informal interpretation of formal international law

Informal interpretation of formal international law refers to the practice of private entities or individuals interpreting international law by means of soft instruments (including principles, guidelines, codes of conduct and resolutions). Private institutions and civil society have adopted a number of principles and guidelines and other mechanisms to protect human rights in the digital ecosystem.

Industry-led coalitions include the Global Network Initiative (GNI), set up in 2008 as a collaborative project of Internet companies including Microsoft, Google and Yahoo. The GNI Implementation Guidelines provide detailed guidance to ICT companies on how to implement the UN Guiding Principles on Business and Human Rights Principles, and provide a framework for collaboration between companies, NGOs, investors and academics. They set out specific guidelines

[63] John Ruggie describes his experience when he formally introduced the Guiding Principles to the United Nations Human Rights Council requesting for endorsement and in response, the Algerian ambassador took the floor and say that governments could not endorse a normative text that they did not negotiate themselves, proposing to submit the Guiding Principles to an inter-governmental process. John Gerard Ruggie, *Just Business: Multinational Corporations and Human Rights (*W. W. Norton & Company, 2013), at xlix.

[64] Full text is available from: https://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf

[65] UN General Assembly Resolution 56/183 (21 December 2001).

on how participating companies should respond to Government requests that might hinder or restrict individuals' rights to freedom of expression and privacy.

NGO-led international coalitions have also been active. The Internet Rights and Principles Coalition is a multi-stakeholder group inspired by civil society that aims to raise the profile of human rights in the Internet Governance Forum. It was formed by merging two coalitions: the Dynamic Coalition on an Internet Bill of Rights, and the Dynamic Coalition on a Framework of Principles for the Internet. The Internet Rights and Principles Coalition has developed a Charter on Human Rights and Principles for the Internet which reflects the structure of the Universal Declaration of Human Rights (UDHR).[66] A separate international coalition of non-governmental organizations launched the Manila Principles of Intermediary Liability, which establish baseline protection for intermediaries in accordance with freedom of expression standards.[67] The Manila Principles aim to encourage the development of interoperable and harmonized liability regimes that can promote innovation while respecting users' rights in line with the UDHR, the International Covenant on Civil and Political Rights (ICCPR), and the United Nations Guiding Principles on Business and Human Rights. A group of civil society organizations have also been involved in the African Declaration on Internet Rights and Freedom, which builds on existing African human rights documents.[68]

Additionally, individuals have contributed to the interpretation of formal international law. The United Nations Human Rights Council appoints Special Rapporteurs, independent experts who conduct human rights inquiries and 'standard-setting activities'.[69] In the area of freedom of expression, some of the most important work of the Special Rapporteur has been to clarify the precise nature of the right through what Mendel describes as standard-setting work. Though their conclusions are not legally binding, Mendel has described the work by Special Rapporteurs as having persuasive force particularly on what State must do to comply with their international legal obligation.[70] He notes, for example, that the European Court of Human Rights has referred to the Joint Declaration by four International Mechanisms for Promoting Freedom of Expression (the United Nations Special Rapporteur on freedom of opinion and expression, the Organization for

[66] The Dynamic Coalition is a multi-stakeholder partnership based at the Internet Governance Forum. It is an open network of individuals and organizations.

[67] See: https://www.manilaprinciples.org/.

[68] See: http://africaninternetrights.org/.

[69] Toby Mendel, 'The UN Special Rapporteur on freedom of opinion and expression: progressive development of international standards relating to freedom of expression' in Tarlach McGonagle and Yvonne Donders (eds), *The United Nations and Freedom of Expression and Information* (Cambridge University Press 2015), 248-257.

[70] Ibid, 248-257.

Security and Co-operation in Europe's Representative on Freedom of the Media, the Organization of American States' Special Rapporteur on Freedom of Expression, and the African Commission on Human and Peoples' Rights' Special Rapporteurs on Freedom of Expression and Access to the Internet).[71]

3.5.4. Informal agreements by public-private institutions

Public-private institutions have been described as 'intergovernmental undertakings which assume private dimensions by acting through institutions that are based in private law, such as firms and associations'.[72] As an example, Benvenisti cited the Global Fund to Fight Aids, Tuberculosis and Malaria. A Swiss foundation, the Global Fund includes delegates from least developed countries, NGOs, and private donors.

The Internet Corporation for Assigned Names and Numbers (ICANN) is another example. ICANN is a non-profit organization incorporated in the United States.[73] It has established a Cross Community Working Party on corporate and social responsibility to respect human rights, which seeks to map and understand and address ICANN's corporate and social responsibilities. The Working Party has mapped the rights in question: right to privacy, right to freedom of association, economic, social and cultural rights, right to freedom of expression, right to security, equality and non-discrimination, and due process.

Further, ICANN has established a dispute resolution process that has its own enforcement mechanism. The Uniform Domain Name Dispute Resolution Policy (UDRP) provides a mechanism for resolving disputes related to the registration of Internet domain names. The World Intellectual Property Organization's Arbitration and Mediation Center and National Arbitration Forum administer domain name disputes in accordance with the "Rules for Uniform Domain Name Dispute Resolution Policy". The remedies it provides for are cancellation of a domain name, or transfer of

[71] Ibid, 264-265. Specifically, the author cites: *Editorial Board of Pavoye Delo and Shtekel v. Ukraine*, where the Court quoted the 2005 Joint Declaration regarding the protection that should be afforded to freedom of expression online; *Yildirim v. Turkey*, where Judge Pinto De Albuquerque's concurring opinion that the wholesale blocking of websites could never be justified relied in part on the 2011 Joint Declaration; and *Youth Initiative for Human Rights v. Serbia*, where the Court quoted parts from 2004 Joint Declaration and 2006 Joint Declaration.

[72] Eyal Benvenisti, 'Towards a Typology of Informal International Lawmaking Mechanisms and their Distinct Accountability Gap' , 301.

[73] In 1983, the US Government selected the Stanford Research Institute (SRI) to manage the new DNS and operate the root server. In 1991, the management of DNS and root server was put out to competitive tender and the work was outsourced to Network Solutions Inc.

the domain name to the complainant. In practice, domain registrars all have an accreditation agreement with ICANN (the registrar accreditation agreement), and the domain name dispute resolution system enjoys a self-contained enforcement mechanism which enforces panel decisions.

3.5.5. Procedures implemented by private entities

Many private businesses in the digital information ecosystem monitor and regulate themselves. These businesses have created a new body of rules, practices, and processes that aim to codify, monitor, and certify their compliance with labour, environmental, human rights or other standards of accountability.

In a number of cases, individual users have acted as a community to resolve problems in the digital ecosystem. This form of self-regulation can be traced back to Web 2.0, which enabled 'crowdsourcing'. The user community also made Wikipedia possible, by cooperating in the production of its articles. Through joint drafting and discussion of Wikipedia rules, users created guidelines to deal with a range of issues, including reversion practices, mediation of disputes, and the blocking of individual users. These rules emerged organically from below and were not dictated by a central authority. Additionally, the Arbitration Committee (Wikipedia's 'supreme court'), a small group of trusted users, act as the final arbiters of disputes. Zittrain notes that these Wikipedia power-users and the accommodating technology constitute a form of self-help group that can resolve problems without invoking the machinery of government regulation or corporate intervention.[74]

In addition to self-monitoring, third parties can act as monitors. An example is the Internet Watch Foundation (IWF), a hotline based in the United Kingdom to which the public and industry professionals can report potentially illegal online content. Illegal content is then taken down by Internet service providers who are members of IWF.

To implement their services, third-party entities such as IWF rely on 'notice and takedown', also known as conditional liability or 'safe harbour'. This method exempts intermediaries from liability for third party content provided the intermediary removes content when informed that it is illegal.[75] The approach can be criticized on the grounds that it places intermediaries in a quasi-judicial position, because they become responsible for evaluating the legality of content.

[74] Jonathan L. Zittrain, 'The Fourth Quadrant', 78 *Fordham Law Review*, 2781.

[75] This approach is furthered divided into two: vertical approach applying to certain types of content such as copyright infringement (US, Digital Millennium Copyright Act) and horizontal approach where different levels of immunity are granted depending on the type of activity at issue (EU E-Commerce Directive).

An alternative model is called a 'notice-to-notice procedure'. This model can be used in cases that do not involve serious criminality (such as child sexual abuse images, or incitement to discrimination, hostility and violence, which are prohibited under international law).[76] Under the notice-to-notice model, a business entity that receives notice of alleged wrongdoing informs the content creator, who is expected to remove the content or resolve the issue with the complainant. It shifts responsibility of evaluating the legality of the content to the user (the generator of content or the complainant).

4. Identifying human rights actors in the digital information ecosystem

It is important to make an overall assessment of who is who and who does what in the digital information ecosystem. However, the mere fact that an actor has a critical function in that ecosystem does not amount to having the status of a subject of international law nor imply that the actor has duties or responsibilities under international human rights law. Identifying actors who do have such duties cannot be done by simply listing all the actors with a role in the digital ecosystem (see the sections above). In the words of Bianchi: "Once the safe harbor of the positivistic doctrine of the 'subjects of international law' is left behind, one finds oneself sailing in uncharted waters, where a primarily descriptive approach is hardly adequate to make up for the lack of theoretical underpinnings to the doctrine of the 'actors of international law'".[77] We need to find out how we can sail these uncharted waters.

How can we determine which actors in the digital ecosystem are actors in the international human rights system? This entails a more in-depth discussion about how State and non-State actors in international human rights law are identified. We therefore begin by discussing the identification of State and non-State actors for the purposes of international human rights law, and go on to ask whether assessing human rights treats posed by functions of digital ecosystem can be applied to identify human rights actors in the digital ecosystem.

4.1. State and non-State actors in the international human rights system

To a certain extent, international human rights law follows the traditional State-centric approach of international law. The parties to international human rights treaties are States, and those treaties assign the primary responsibility for promoting and protecting human rights to State parties. This State-centred approach recognizes human rights actors in the following terms: (1) private individuals

[76] Article 19, 16 – 17.

[77] Andrea Bianchi, 'The Fight for Inclusion: Non-State Actors and International Law', at 40.

and groups are only actual or potential victims; (2) States are both violators and protectors of the rights of the populations under their jurisdiction; and (3) States and international organizations promote human rights by monitoring the conduct of all States.[78]

The purpose of international human rights treaties is to protect individuals and groups from unlawful violations of their rights. In consequence, the human rights-based approach distinguishes actors who are 'duty-bearers' (who have obligations or responsibilities to respect, promote and protect human rights) and actors who are 'rights-holders' (individuals or social groups who are entitled to exercise those rights and to protection). 'Duty-bearers' are not limited to States; as we have seen, other actors such as business entities have certain responsibilities to respect human rights.[79] In this context, a widening discussion of the role and responsibilities of non-State actors (actors other than States) has taken shape quite recently in the international human rights law field.

Who are non-State actors in the context of international human rights law? Apart from their negative definition as 'actors other than States', no single specific definition of non-State actors has been agreed upon. Depending on their characterization, they include a wide variety of entities: transnational corporations and private companies, international organizations, non-governmental and civil society organizations, rebels and insurgents, and individuals. We do not attempt here to describe or assess historical discussions of the definition of 'non-State actor' and do not attempt to produce our own definition.[80]

The term 'non-State actors' is not the only term used to describe entities that are not States. Some commentators speak of 'non-state perpetrators' to refer to non-State actors (such as rebels and liberation movements) whose actions would be considered violations of human rights if they were State actors.[81] McCorquodale uses the term 'individuals' to refer to natural and non-natural

[78] Zehra F. Kabasakal Arat, 'Looking beyond the State But Not Ignoring It' in Zehra F. Kabasakal Ara, Peter Juviler and George Andreopoulos (eds), *Non-State Actors in the Human Rights Universe* (Kumarian Press, Inc), 26.

[79] United Nations Guiding Principles on Business and Human Rights Implementing the United Nations "Protect, Respect and Remedy" Framework.

[80] On defining non-State actors, see Philip Alston, 'The 'Not-a-Cat' Syndrome: Can the International Human Rights Regime Accommodate Non-State Actors?' in Philip Alston (ed), *Non-State Actors and Human Rights* (Oxford University Press 2005), 14-17.

[81] Herbert F. Spirer and Louise Spirer, 'Accounting for Human Rights Violations by Non-State Actors' in Zehra F. Kabasakal Arat, Peter Juviler and George Andreopoulos (eds), *Non-State Actors in the Human Rights Universe* (Kumarian Press, Inc), 44.

legal persons, relying on the fact that natural persons form groups due to common interests.[82] In his terminology of individuals, he includes that natural persons and legal persons composed of individual persons (such as businesses and non-governmental organizations) are entities that are not States.

Irrespective of the terminology used, it is clear that, merely by discussing non-State actors in international human rights law, we are moving away from the State-centred approach, towards one that focuses on protecting the rights of all individuals against violation by any organ of the society. Arat proposes a human-centred framework which identifies the following actors who can violate or protect the rights of individuals: State agencies, private individuals and groups, foreign State agencies, foreign private individuals and groups, international government organizations, transnational corporations, and NGOs.[83]

Developing Arat's approach, I propose to shift the focus from identifying specific types of actor who violate or protect rights to identifying specific *functions* that violate or protect rights. In other words, I propose that actors should be assessed according to their functions. By assessing functions and how functions interact in the digital information ecosystem, we can more clearly understand their negative (or positive) impacts on enjoyment of human rights. In this regard, according to Andrew Clapham:

> "We should indeed *examine their activity and their interaction with states and others* to determine the duties and rights that states have fixed them with. […] Such an examination will reveal the concern of states to address the *behaviour of non-state actors that threatens international human rights*.[emphasis added]"[84]

If core functions in the digital information ecosystem threaten (or protect) human rights, the actors that perform them may be elevated to the status of 'human rights actor' and be held responsible for negative impacts on rights that arise from the conduct of their functions. Furthermore, States should recognize that these human rights actors and their functions represent a potential threat (or protect) to the enjoyment of human rights and exercise their obligation to protect third parties from harm and restrain third parties from doing harm.

[82] Robert McCorquodale, 'The Individual and the International Legal System' in *International Law Beyond the State: Essays on Sovereignty, Non-State Actors and Human Rights* (CMP Publishing 2011) , 249.

[83] Zehra F. Kabasakal Arat, 'Looking beyond the State But Not Ignoring It' in Zehra F. Kabasakal Ara, Peter Juviler and George Andreopoulos (eds), *Non-State Actors in the Human Rights Universe* (Kumarian Press, Inc), 28-30.

[84] Andrew Clapham, 28. Emphasis added.

4.2. Threats to human rights: controlling the flow of digital information

What impacts do the functional components of the digital information ecosystem have on the exercise of rights? More specifically, when implemented or during implementation, how do they promote or infringe enjoyment of human rights? Each core function in the digital information ecosystem occupies a specific role, such that in its absence the ecosystem cannot operate and individual users cannot use its services to exercise their rights online. The tricky question is whether particular components can negatively impact, threaten or violate human rights, if they are designed differently or used in a different way.

The main online threats to human rights are associated with the flow and the life cycle of digital information. The ecosystem is centred on creating, transmitting, processing or otherwise manipulating digital information. Rights on line are exercised by accessing, using or being informed of the whereabouts of digital information. Since all activities online are based on digital information, the key test for assessing whether certain functions pose a threat to rights, is 'who has control over information?'

'Control of digital information' is often discussed as if it means the same as 'control of the Internet'. With the rise of the Internet, the power and control exercised in the digital environment has been central focus of various discussions. Who controls the Internet has often been discussed, using a variety of terminologies. We therefore start by examining terms and definitions.

Some commentators use the term 'gatekeeper' to describe the entities that regulate the Internet.[85] Zittrain identifies two kinds: traditional gatekeepers who enforce and regulate the conduct of third parties; and technological gatekeepers who regulate individual behaviour indirectly by changing technology.[86] Others speak of 'points of control', meaning any public or private actors who play a strategic role in a particular area. Tim Wu coined the term 'master switch' and refers to entities such as Google, as the Internet's great switch and the Web's current custodian.[87]

Laidlaw, who calls Internet gatekeepers 'Internet information gatekeepers', argues that they are capable of impacting democracy in the way that public institutions traditionally did, because of the

[85] For an overview of the history and trajectory of gatekeeping, beginning with defamation, copyright infringement and peer-to-peer networks, see Jonathan Zittrain, 'A History of Online Gatekeeping ', 19 *Harvard Journal of Law and Technology*.

[86] Ibid , 255-256.

[87] Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Vintage, 2011), 280.

kinds of business they do and the technology they apply.[88] Based on the extent of the control that gatekeepers exert, their democratic significance and the influence over the public sphere of the information they control, Laidlaw identifies Internet information gatekeepers at three levels: 'micro-gatekeepers' (content moderators, such as interactive website platforms); 'authority gatekeepers' (websites that have high traffic and high information flows, like Facebook); and 'macro-gatekeepers' (ISPs and search engines).[89] While this spectrum may reflect the situation at a particular time, it remains a challenge to define information that has democratic significance or assess impact on the public sphere. Moreover, irrespective of where a gatekeeper stands on the proposed spectrum, all entities in the digital information ecosystem have an equal capacity to restrict and filter content, while their impact is subject to the dynamic evolution of the digital ecosystem.

Once again, it makes sense to define 'control' and 'controller' in terms of technical function. In computer science, a controller is a hardware device or a software program that manages or directs the flow of data between two entities. Controllers may be cards, microchips or separate hardware devices for controlling a peripheral device. In a general sense, a controller can be thought of as something or someone that interfaces between two systems and manages communications between them. Taking these definitions into account, controllers in the context of the digital ecosystem can be described as entities that have the capacity to direct or restrict the flow of digital information and the interfaces between systems, namely, various forms of access to different parts of the digital ecosystem.

We can conclude that, in the digital information ecosystem, all components have a capacity to control the flow of digital information. All critical functions in the digital ecosystem have a dual purpose: to facilitate activities in the digital ecosystem; and to control the flow of digital information. The actors associated with those functions have the capacity and the power to control the flow of digital information, to determine where information goes to and how fast it travels, and to prevent information from reaching intended recipients. By controlling the flow of digital information, those actors also control the behaviour of individuals that use the digital ecosystem.

4.3. Functions in the digital information ecosystem that threaten human rights

The potential threats to human rights that elements of the system pose are assessed below. The examples provided are not exhaustive. In Chapter 3, we analyse in more specific terms how

[88] Emily B. Laidlaw, 'A Framework for Identifying Internet Information Gatekeepers', 24 *International Review of Law, Computers and Technology*, 7.

[89] Ibid.

providers and their functions can affect the flow of digital information. Chapter 3 also discusses how the life cycle of digital information can be used to track the flow of digital information.

4.3.1. Provision of products and services

The provision of different products and services is central to the architecture of the digital ecosystem, affects several layers of the system, and can both assist and hinder the activities of individuals online.

We look at different layers of the digital ecosystem to show how providers of products and services (devices and software, network connectivity, web-based services and certification) can exercise control over the flow of digital information.[90]

First, provision of devices and software, for example, includes the manufacture of routers (processors that connect two networks and relay data from one network to another). Routers send information packets (information broken down into smaller units) to their destinations; if an error occurs, they reject the packet, return it to the sender, log information about it, and set off an alarm to notify the user. Simply put, ordinary routers look at the destination address of each data packet and choose the best way to send it to its correct destination. More sophisticated routers can modify information by changing the destination address, send the packet to another destination, and modify filtering rules. These routers do deep-packet inspection, a function that inspects information and decides whether it should be censored according to rules that are embedded and coded in the technology. An analogy can be made with passport control at a frontier, where (depending on who you are) officials (the controller) decide to permit entry on the basis of the country's laws.

Other hardware and software devices include switches, LAN cards, and firewalls, which constitute a 'network node' connecting other channels into which digital information flows. When digital information travels through these channels, it relies on information that provides source and destination addresses (logical addresses or IP addresses), which are often digitally embedded. Specific layers of the ecosystem facilitate addressing and routing of data.[91] Devices may have embedded software programmed to filter or screen out content. On this ground, Zittrain correctly predicted that "control over software rather than control over the network will be a future battleground for Internet regulation".[92]

[90] Of the seven layers of the OSI model, the following are relevant: physical layer (layer 1), network layer (layer 3), transport layer (layer 4), and application layer (layer 7).

[91] Network layer and transport layer (layers 3 and 4 of OSI model).

[92] Jonathan Zittrain, 19 *Harvard Journal of Law & Technology*, 254, 294-297.

Second, network connectivity is mainly assured at the physical layer (layer 1), where devices access the network's wireless or fibre-optic infrastructure to send data to other systems. The physical layer determines how digital information is physically sent through the network, using mediums such as coaxial cable, optical fibre, or copper wire. Actors that provide access to the physical network can influence how digital information is distributed and can regulate how information flows. For instance, certain providers that operate an Internet Exchange Point (IXP, a physical infrastructure through which network connectivity providers exchange Internet traffic between their networks) control the international flow of information. Providers also control bandwidth (channel capacity), which determines how many users can communicate and what type of content they can access.

Third, the provision of web-based services, including applications and platforms, is delivered in the application layer, the closest to individual users. This is where web browsers, emails and other client applications familiar to users operate. In general, the application layer regulates users' behaviour. It applies rules on how users can behave and sets conditions on users' access to cyberspace. Lessig suggests that technical solutions may be replacing or displacing law, because programing and codes dictate and regulate the behaviour of users in the digital sphere.[93]

Two examples show how the application layer exerts control over the flow of digital information. In the twenty-first century, most web-based applications are provided through the 'cloud'. Cloud-computing services place personal data and information on remote servers, and control over data can therefore be exercised by those that have (lawful or unlawful) access to them. Users can easily lose control over their data and control shifts to the entities that manage cloud computing services. Additionally, it is in this last layer that information can be scanned. In October 2016, it was allegedly reported that Yahoo! had built software at the request of US intelligence officials that would scan users' email accounts for specific information. It is also in this layer that control over access to different parts of the online platform is exercised. Administrators in any system have the authority to restrict and alter access rights of users and systems.

Fourth, certification providers, who manage identities, are in a position to control information on identities or identity credentials. An identity credential is data that is used to authenticate the claimed digital identity or attributes of a person. It typically contains a 'unique identifier' (such as a name, user ID, account number, social security number, driving licence, passport, etc.) and relevant

[93] Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0 (*Basic Books 2006).

identity attributes that describe or define the person in sufficient detail for the purpose at hand (address, title, gender, date of birth, etc.).

In many countries that have an advanced electronic commerce ecosystem, digital identification is a basic requirement for performing any activities online. In countries with strict encryption and specification requirements, users are unable to purchase goods online without a mobile number registered under real-name or a digital certification registered with accredited certification authority. These barriers not only restrict commercial activities but have a significant impact on the user's capacity and ability to freely express himself or herself in the digital sphere and enjoy rights to which they are entitled. In many States, for instance, laws require the provision of identification at cybercafés.[94] In States where computers and mobile devices are rare, individuals have no choice but to rely on public computers in such cybercafés.

Financial intermediaries in the online industry (such as credit card companies) critically influence transactions online.[95] They control entities on the digital information ecosystem whose business relies heavily on remote payment methods. For example, HavenCo, a one person company was established in an abandoned concrete platform in the North Sea which was claimed by an individual as an independent Statem calling it the "Principality of Sealand".[96] Sealand has not been officially recognised by any established sovereign state. Operating outside the jurisdiction of any State, HavenCo provided computer space for unlawful activities. Because financial intermediaries were unwilling to cooperate with it, however, the company could not be sustained and was forced to close down.

4.3.2. The function of user of the digital information ecosystem

Control over the information flow can also be exercised by controlling those who use the products and services that other actors provide. In contrast to the Internet-based industry, other media industries are all predicated on control of customers. For instance, the radio and television industry controls the information that customers will receive, including advertisements. By contrast, the

[94] For instance, India, Information Technology (Guidelines for Cyber Cafes) Rules 2011. See, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/23/40, para. 68).

[95] Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World (*Oxford University Press, 2008), at 76 – 77. An example is given where cigarette industry faced difficulty in selling cigarettes online after the credit card companies accepted to not allow transaction of sale of cigarettes through online shops. This eventually made it burdensome for purchasers to buy online cigarettes.

[96] Ibid , at 68-71.

Internet allows individual users to choose what they access; users can skip from website to website in ways that are not dictated by a content provider, and can control what content reaches their computers. Some international civil liberties organizations that focus on regulating the access of minors to pornography contents argue that end-users should censor and filter content, on the grounds that this raises freedom of expression concerns arising from government censorship.

Furthermore, any system can be managed and controlled by a legal entity or the individual, allowing individual users to perform the role of administrator. Administrators charged with managing WiFi also have the authority and power to regulate access to the network's infrastructure, which gives users access to the Internet. For instance, in a company or university, administrators have authority to limit users' access to the Internet in a given space or time. Under the direction of the law faculty, administrators at the University of Chicago Law School disconnected in-class Internet access when students had classes.[97]

4.3.3. Allocation of resources

The allocation of resources (domain names and IP addresses) can also serve to control information. In addition to information as texts, pictures, video or audio, non-conventional forms of digital information exist, that are less familiar to ordinary users. One such is a website's address (its Internet domain name). Information can be controlled and filtered by manipulating the domain name system. For instance, Cleanfeed uses the domain name system to block a part of the servers and does not block the entire IP addresses in order to avoid over blocking. In simple terms, participating Internet service providers are given a list of IP addresses to filter and the ISP automatically filters the website without knowledge of what it contains. Canada has implemented Cleanfeed to block access to child pornography.[98] France's cybercrime unit uses a similar technology to block webpages that promote terrorism on the Internet.[99]

Domain name registrars (who manage the reservation of Internet domain names) maintain central databases called WHOIS, which store information, about the registered users of domain names (including their contact details) and the expiry dates of domain names. WHOIS databases are

[97] UChicagoNews, 'University of Chicago Law School eliminates Internet access in some classrooms', 11 April 2008. At: https://news.uchicago.edu/article/2008/04/11/university-chicago-law-school-eliminates-internet-access-some-classrooms.

[98] See: https://www.cybertip.ca/app/en/projects-cleanfeed.

[99] Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.

widely available to the public and reveal information about those who have registered domain names. This has raised concerns about privacy, freedom of expression, and anonymity.

4.3.4. Creation of technical standards

Technical standards are not normative in nature and do not aim to steer behaviour or determine personal freedom. Yet the effects of technical standards may influence the flow of digital information and freedom to use it. For instance, technical standards may affect access to a network or its content. For example, China's WLAN Authentication and Privacy Infrastructure (WAPI, a national Wireless LAN standard) enforces a closed wireless network that requires all its users to register with a centralized authentication point. Another example was the World Wide Web Consortium's Platform for Internet Content Selection (PICS), which preceded the current Protocol for Web Description Resources (POWDER). Content creators could apply PICS to enable users to filter out unwanted content (blacklisting) or filter out all but trusted content (whitelisting). These standards made it possible to prevent digital information from reaching its intended audience.

The Internet Protocol (IP) is another technical standard that can have an impact on human rights. Currently, Internet Protocol version 4 (IPv4) is giving way to Internet Protocol version 6 (IPv6), because it has run out of addresses. IPv6, developed by the Internet Engineering Task Force, will provide sufficient IP addresses to assign a unique IP (for identification and location) to every device on the Internet, allowing individuals to use their laptops or smartphones to communicate with and remotely control home appliances via machine-to-machine communication. IPv6 nevertheless raises privacy and security concerns because it will allow individual devices and their location to be uniquely identified and make it easier to track behaviour online.

4.3.5. Creation of laws and non-laws

International law can be described as a set of instruments and norms that change and regulate the behaviour of States. In general, laws are strongly normative in nature, in that they govern the behaviour of the societies which established them. In the digital ecosystem, laws are similarly created to regulate and enforce behavioural norms, alongside informal or non-laws with quasi or non-judicial enforcement mechanisms. These standards and protocols regulate every aspect of the digital ecosystem and therefore influence how individuals access and use digital information.

5. Assessment of human rights actors in the digital information ecosystem

All human rights actors that perform functions critical to the operation of the digital information ecosystem are in a position to control the flow of digital information, and therefore negatively impact (or promote) enjoyment of individual rights online. Additionally, by virture of that control, the same actors are in a position to regulate the behaviour of individual users in the system; their controlling function has a legal effect. In the current digital society, within the confines of the ecosystem, private entities or third parties have established and implement internal codes of conduct and procedures, despite the fact that the legitimacy of the procedures and those responsible has never been made clear. It is therefore pertinent to ascertain whether the human rights actors in question have the legitimate authority and status to create norms and rules that govern and regulate the behaviour of individual users or other actors, and whether those norms and rules are legitimate.

5.1. Question of legitimacy

It is evident in practice that certain actors carry out functions within the digital information ecosystem that are critical to the realization and enjoyment of human rights online; some of these functions were traditionally undertaken by States. It is equally clear that the fact that this is so does not mean that the actors concerned have legitimate authority to perform the functions in question.

'Controller' functions (as described in section 2.4.3) are mostly performed by non-State entities. They are not therefore subject to public service norms of professionalism or (at least directly) international human rights treaties. Their responsibilities and conduct often lack transparency. As a result, individual users do not know what standards they can depend upon or what forms of redress they are entitled to claim. They lack appropriate mechanisms to appeal against decisions and actions taken by entities that exercise controlling functions. For all these reasons, it is desirable to clarify the extent to which human rights actors in the digital information ecosystem have legitimate authority under national and international law to carry out their functions.

Achieving that clarity is more difficult where experts in technical standardization bodies establish technical standards in their personal capacity or as representative of government. Both public and private organizations are responsible for technical standard setting. They include corporations, trade associations, governments, professional associations, and standards organizations (such as the International Organization for Standardization, ISO). The fact that several have overlapping functions may create checks and balances. However, As Murray points out, it can also mean that no one body has authority to change an Internet standard or be accountable for it.[100]

[100] Andrew Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge-Routledge, 2007), 92.

The composition of bodies that create technical standards is important because technical design decisions and technical standards can have specific and harmful effects on public policy and individual rights, especially if they are not addressed early on.

> "Consideration of policy issues must happen early in the design process... If policy concerns are not raised until after a standard is finalized, or after products are deployed, the chance of constructive change is very low. Legislative or regulatory fiat cannot inject into a service or product technical capabilities that were not designed in the first place, and can often at best only restart a lengthy standards design process."[101]

However, standard-setting bodies operate largely outside of public scrutiny and receive little input from public interest groups or public policy makers. Technical standard-setting bodies should increase their procedural openness and transparency and develop procedures for identifying whether public policy concerns may be affected.

Technical standards agencies have decided to integrate privacy in the design requirements for all Internet standards, a policy called 'privacy by design'. For instance, the Internet Engineering Task Force recently indicated that privacy will be considered before protocols are designed or updated at all layers of the Internet. However, they do not value privacy as a human right per se. Instead, they see it as an issue that puts at risk the functioning of the network.[102] For the technical community, in fact, protection of privacy matters because it is understood as a necessary condition for maintaining user's trust. The core architecture of the digital network and the growth of the Internet depend on the presumption of trust and threats to privacy impact the level of trust placed by users. Although the technical community and human rights actors therefore have a similar *objective* with respect to privacy, the technical community's *motivation* is different. As a result, technical standards introduced to protect privacy may have a negative or positive effect on privacy as a human right. Should technical standardization bodies be permitted to work on privacy related matters without considering its human rights dimension and without consulting the human rights sector? This is essentially a legitimacy issue.

A different legitimacy question arises in relation to process. Many entities run monitoring or complaints 'hotlines', and several third-party bodies monitor and enforce non-judicial decisions in the digital ecosystem. These private sector organizations are not judges or courts: they are not

[101] John B. Morris Jr. 'Injecting the Public Interest into Internet Standards', in Laura DeNardis (ed) *Opening Standards: The Global Politicis of Interoperability* (The MIT Press 2011), at 7.

[102] Adamantia Rachovitsa, 'Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue', 24 *International Journal of Law and Information Technology*, 381-382.

officially authorized to make determinations of legality, nor are they subject to formal public controls or accountable to the public. A famous case shows why this is a concern. In response to a complaint, the Internet Watch Foundation added a page to its blacklist of alleged child sexual abuse content. The Wikipedia page in question showed the album cover of a rock bank and featured the image of a naked 10 year-old girl. On receiving the blacklist, IWF members blocked access to the page. The blocking methods used caused technical problems and as a result, the users who accessed Wikipedia page experienced slower connection speeds.[103]

The practices of standard setting entities when they establish standards also raise questions of legitimacy. The following examples concern possible conflicts of interest. The first concerned telecommunication standards developed by the International Telecommunication Union. Until 2001, all standards had to be approved by Member States before they became official. As communications technologies multiplied, this practice was changed and the Alternative Approval Process (AAP) was adopted. This enables standards to be approved by members of the study group that developed them, essentially the private sector. The second case relates to the Internet Engineering Task Force (IETF). Under its rules, each new proposal for specification is reviewed, revised and initially published as a ‘Request for Comment’ (RFC), until it reaches a certain level of maturity and becomes an Internet standard. To be adopted as an Internet standard, the specification must be of the highest technical quality and receive widespread support from the relevant technical community. In addition, crucially, a third requirement must be met: the IETF assess the interests of all affected parties as well as the specification’s contribution to the Internet. These examples demonstrate, first, that standards are often established with the interest of private entities in mind and driven by those interests, and second, that procedural steps can be taken to balance such forms of bias, including conflicts of interest. It is therefore important to explore the safeguards standards-setting processes put in place to ensure that public interest and human rights principles are taken into account.

Legitimacy issues arise in a number of other areas. What can be emphasized is that non-State actors exercise functions *de facto* do not automatically acquire legitimate authority to exercise those functions. The international human rights system should, first, put in place rules and safeguards to monitor human rights actors in the digital information ecosystem and, second, should identify and make clear the human rights obligations of those actors. In this regard, two main points should be

[103] Emily B. Laidlaw, ‘The responsibilities of free speech regulators: an analysis of the Internet Watch Foundation’, 24 International Journal of Law and Information Technology, 312-345.

considered from the perspectives of the international legal system and the digital information ecosystem.

From the perspective of the international legal system, we cannot ignore the fact that States remain the primary actor in international human rights law. States clearly have the primary obligation to respect, protect and fulfil human rights. It is with the consent of States that international law is created and implemented. States also define the entitlements and duties of non-State actors under international law. Most important, individuals or groups whose rights are threatened and violated by non-State actors very often cannot easily claim their rights through judicial proceedings or complaint mechanisms. In the absence of formal recognition by States, the enforcement of international law is almost non-existent in practice.

From the perspective of the digital information ecosystem, we cannot ignore the fact that the ecosystem was not designed to be centrally controlled. It is based on open architecture and the trust of users. The underlying design allows end-users to determine what information they receive and what services they benefit from. Centralized control or regulation of the Internet would undermine its fundamental identity. For this reason, regulation of the digital ecosystem is not proposed as a solution. States should implement their obligation to protect individuals from third parties and, to do so, should establish safeguards and procedures to monitor that all human rights actors in the digital ecosystem abide by human rights principles and respect rights enshrined in international human rights treaties. However, to protect human rights in the digital information ecosystem legitimately, without central regulation, the commitment to comply with human rights principles must come from actors in the ecosystem themselves. They and the ecosystem regime must actively agree that they have defined duties and obligations under international human rights treaties. The question of legitimacy will be resolved when these duties are specified and accepted by human rights actors in the digital ecosystem.

More specifically, these obligations should be defined in terms of the functions of human rights actors in the ecosystem (not their formal status). To assess the nature and extent of their obligations, I propose using the life cycle of digital information as a framework. Each action in the digital life cycle is specific and the actors involved therefore need to address them one by one. Subsequent chapters of this thesis address how human rights issues occur in the course of the digital life cycle: pre-stage; creation; transmission; storage; collection; process and disposal. Before examining the obligations of human rights actors by their function, we first consider the emergence of new human rights actors in the digital ecosystem, whom States should recognize.

5.2. A new typology of human rights actors

The dynamic nature of the digital information ecosystem and the way it has evolved with little State involvement has created a new typology of human rights actors. Since the ecosystem continues to evolve and as new technologies are developed, new human rights actors will emerge adding to the actors enumerated below. It is critical that States recognize these human rights actors, and that individual rights holders are also aware of their functions, and the impact of those functions on our rights. This section outlines the new typology of actors in the digital ecosystem. Trans-governmental institutions, international agencies, industry associations, international Internet institutions, and individuals are each considered separately.

5.2.1. Trans-governmental institutions

While States remain the most important actors in the international legal system, in some international forums, accredited delegations of States as well as non-accredited representatives of Governments engage in law-making activities. Anne-Marie Slaughter explains this phenomenon as disaggregation of States into component institutions due to the growing need of different domestic government institutions to engage in activities beyond their borders, often with their foreign counterparts.[104]

> "Looking at the international system through the lens of unitary states leads us to focus on traditional international organizations and institutions created by and composed of formal state delegations. Conversely, however, thinking about states the way we think about domestic governments – as aggregations of distinct institutions with separately roles and capacities – provides a lens that allows us to see a new international landscape."[105]

Trans-governmental institution, also called 'harmonization networks', are international networks of national public regulatory authorities that collaborate to harmonize their rules or set standards or other norms.[106] Slaughter defines 'harmonization networks' as networks that bring regulators together to ensure that their rules in a particular substantive area conform to a common regulatory

[104] Anne-Marie Slaughter, *A New World Order* (Princeton University Press, 2004), 12.

[105] Ibid, 13.

[106] Ayelet Berman and Ramses A. Wessel, 'The International Legal Form and Status of Informal International Lawmaking Bodies: Consequences for Accountability' in Ramses A. Wessel, Joost Pauwelyn, and Jan Wouters (eds), *Informal International Lawmaking* (Oxford University Press 2012), 35.

standard.[107] They are composed of national government officials, who are elected or appointed by elected officials. They set standards in areas of international public policy and, by avoiding the rigidities and formality of international legal forums, tend to be overlooked as actors of international law.[108]

Such institutions are sometimes called 'standard development organizations', reflecting their primary role. Examples in the international arena include the International Organization for Standardization (ISO), an independent, non-governmental international organization with a membership of 163 national standards bodies; and the International Electrotechnical Commission (IEC), a non-profit, non-governmental standard-setting organization composed of members (called national committees) who represent national electrotechnical interests.

While some trans-governmental institutions engage in norm-setting or standard-setting, others are forums for the exchange of information and experience. These trans-governmental institutions are called 'international cooperation institutions'. One example is the Asia Pacific Privacy Authorities (APPA), the principal forum for privacy and data protection authorities in the Asia Pacific region. APPA forms partnerships and exchanges ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints.[109] Privacy and data protection authorities based in the Asia Pacific region are eligible for APPA membership if they are: an accredited member of the International Conference of Data Protection and Privacy Commissioners; a participant in the APEC Cross-border Privacy Enforcement Arrangement; or a member of the Global Privacy Enforcement Network. These and similar regional data protection forums are not strictly intergovernmental organizations because they were not created by treaty; nevertheless, their members are State data protection commissioners established and appointed under national laws.

5.2.2. International agencies

While there is no generally agreed definition of 'international organization', these institutions are generally defined by four criteria: they are created by States, based on treaty, have at least one organ, and possess an autonomous will ('*volonté distincte*') distinct from that of its member States.[110] Other criteria include the capacity to adopt norms that apply to its members, possession of

[107] Anne-Marie Slaughter, 20. In addition to harmonization networks, Slaughter identifies 'information networks' and 'enforcement networks'.

[108] Andrea Bianchi, 'The Fight for Inclusion: Non-State Actors and International Law', 56.

[109] See: http://www.appaforum.org/.

[110] Jan Klabbers, *Advanced introduction to the law of international organizations* (Edward Elgar, 2015), 7.

a constitution, and attribution of a legal personality. International organizations that are established by international organizations are referred to as 'international agencies'. International agencies are international bodies that do not derive their existence or mandate from a treaty or cooperation between national agencies, but from the decisions of international organizations.[111] International agencies differ from the special agencies of the United Nations such as the International Monetary Fund which are created by treaties either by the United Nations or have been incorporated into the United Nations system.

International agencies can be set up by one international organization to help attain the objective that organization. The bodies established by the United Nations General Assembly or its subsidiary organs provide the best-known examples of international agencies. For this study, the most relevant agency is the United Nations Conference on Trade and Development (UNCTAD), which is the secretariat of the United Nations Commission on Science and Technology for Development, a subsidiary body of the United Nations Economic and Social Council. International agencies may also be created by two or more international organizations in partnership. Examples include the Broadband Commission for Digital Development, established by the ITU and UNESCO; and the United Nations Group on Information Society, established by several international organizations and agencies to promote WSIS objectives by strengthening their collaboration and developing partnerships among the members of the United Nations Chief Executive Board.

Multi-stakeholder forums are a further type of international agency. This model has been promoted internationally in recent years, and numerous multi-stakeholder initiatives have emerged, notably to address questions of governance. The need for institutionally-inclusive approaches became evident as it became clear that many global concerns could only be addressed through broad cooperation by a wide range of stakeholders (including governments, private businesses, and civil society). The proliferation of international actors also encouraged States to recognize that effective international governance and the development of international law both required wide consultation.[112] Multi-stakeholder approaches are believed to strengthen the effectiveness of processes to create and then implement new formal and informal laws and norms.[113]

[111] Ayelet Berman and Ramses A. Wessel, 44.

[112] Wolfgang Benedek, 'Multi-Stakeholderism in the Development of International Law' in Rudolf Geiger, Ulrich Fastenrath, Daniel-Erasmus Khan, Andreas Paulus, Sabine von Schorlemer, and Christoph Vedder (eds), *From Bilateralism to Community Interest: Essays in Honour of Bruno Simma* (Oxford University Press 2011), 204.

[113] Ibid, 209.

An example in the Internet governance field is the Internet Governance Forum (IGF). The IGF's mandate originates in the Tunis Agenda adopted at the second WSIS in 2005, when State delegates to the WSIS asked the United Nations Secretary General to convene a multi-stakeholder policy dialogue that became the IGF.[114] IGF gathers representatives from government, business, civil society, industry, academia, and international organizations. It differs from other international agencies or subsidiary organs in that it is an ad hoc platform. It has specific work methods, procedures and a small secretariat. It does not take decisions, but debates all the major issues of Internet governance in order to identify areas of common ground that will assist States and other actors to deal with challenges associated with the information society.

5.2.3. Non-governmental organizations: industry associations

Human rights audience tend to identify non-governmental organizations (NGOs) with civil society organizations and civil movements that focus on national and international (human rights) advocacy. However, there exist countless NGOs that have a wide range of vocations, and it is not simple to characterize NGOs in a single definition.[115]

In a broad sense, NGOs are typically private institutions in the form of association, foundations, federation or other unions, founded on the basis national private law, which can be distinguished from business entities because they pursue 'public interest' objectives. Some NGOs have limited and specific objectives. Examples would include labour unions and professional associations. NGOs also include not-for-profit industrial associations that promote the economic interests of profit-making industries.

The NGOs that are of interest to this study include professional organizations, business associations and labour unions. For its purposes, we will consider NGOs to be independent organizations (not established by a government entity or inter-governmental agreement), established under national laws, that are not-for-profit, and whose activities are related to the digital ecosystem. It is understood that not-for-profit industry associations seek to advance the interests of the business entities that are their members. An example of an industry association NGO

[114] Tunis Agenda, para. 72.

[115] For examples of definitions, see for example: (1) ECOSOC Resolution 1996/31, which implements article 71 of the United Nations Charter; (2) The Guidelines for Association Between the United Nations and NGOs, elaborated by the Department of Public Information; (3) The Panel of Eminent Persons on UN Relations with Civil Society; (4) The European Convention on the Recognition of the Legal Personality of International NGOs; (5) The Yearbook of International Organizations, published by the Union of International Associations. See also Ingrid Rossi, *Legal Status of Non-Governmental Organizations in International Law* (Intersentia, 2010), 1-9.

is the Internet Governance Coalition, an industry-led coalition with broad representation from across the Internet ecosystem that campaigns for a safe, secure, open, interoperable, and global Internet, because these characteristics create the underlying foundation for sustainable economic and social development.

5.2.4. International (Internet) institutions

Entities like the Internet Society and the Internet Engineering Task Force blur the boundary between NGOs and private commercial organizations. These entities are not government organizations but 'consortia of persons and companies' that seek to develop Internet industry standards that promote their interests. They have "organically evolved to guide the operation and development of the technical infrastructure that composes the global Internet".[116]

Mueller uses the term "organically developed Internet institutions (ODii)" to describe these bodies.[117] Each was formed because a specific problem with management or development of network protocols emerged that needed resolution but for which no one had responsibility. Usually, an individual would pioneer work on the problem and an institution gradually emerged as he or she sought the input of peers. On the basis of this organic process, Mueller concluded that ODiis represent a movement from State to non-State actors, from closed to more open and participatory processes, and to new kinds of technical expertise.[118] For the purpose of this study, the term 'International (Internet) institution' refers to these organizations and communities.

Although they may both wish to set standards or protocols in the Internet, international Internet institutions differ from trans-governmental institutions in that they are composed of individual experts and members of the business community and were established informally without elected boards or members.

The mandates of these bodies are likely to continue to evolve in a similarly organic way, reflecting the rapid evolution and expansion of information technologies. Bearing this in mind, we look below at three prominent international Internet institutions and their mandates: the Internet Society; the Internet Engineering Task Force; and ICANN.

[116] Internet Society, *Internet Ecosystem: Naming and addressing, shared global services and operations, and open standards development* (February 2014), 5.

[117] Milton Mueller, *Networks and States: The Global Politics of Internet Governance (*The MIT Press, 2010), 217 – 218.

[118] Ibid, 217.

The Internet Society is an international, non-profit, membership organization that promotes expansion of the Internet. It emerged from within the engineering network and was set up to develop and evolve network protocols.

The Internet Engineering Task Force is a large open-access international forum; it is a community of network designers, vendors and researchers who are interested in the evolution of Internet architecture. Its mission is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

ICANN is a private sector organization that manages Internet resources for the benefit of the public.[119] The operation of ICANN and its legitimacy, as well as its governance, were questioned over a long period. Until it recently relinquished its authority, the US government exercised political oversight of ICANN through a contract between ICANN and US government (the IANA contract) which authorized ICANN to perform technical functions of IANA, and an 'Affirmation of Commitment' between the US Department of Commerce and ICANN, which laid out the policy-making tasks that ICANN was to perform. With respect to ICANN's internal structure, a Government Advisory Committee placed US government advisers inside ICANN. Critics suggested that, because this Committee was had an advisory role and did not supervise or regulate, the US Government evaded its responsibility to ensure that lawful due process and human rights were respected.[120]

Further concerns were raised that ICANN's responsibility to maintain the root server should not be controlled by a single State. Its authority over the root of the domain name system and the root of the Internet addressing system permitted ICANN to enforce a variety of policies that were beyond the scope of technical coordination. Whoever stands at the peak of the hierarchy of the system has effective control over the possession and use of identifier resources by all users further down the hierarchy. For instance, ICANN was in a position to control market entry, the prices charged by service providers, and dispute resolutions, among other matters.

5.2.5. Individuals

As described in Chapter 1, individual hobbyists turned business entrepreneurs developed the digital ecosystem. Individuals contributed both to the development of digital technologies and the ecosystem as well as to regulation of the digital space. Individuals play several substantial roles in the digital ecosystem. Individuals and business entities are providers (section 2.3.1), distribute and

[119] In 2005, at the WSIS in Tunisia, the European Union proposed to shift domain name governance from ICANN and the US Commerce Department to a UN-affiliated intergovernmental group.

[120] Milton Mueller, 243.

manage critical Internet resources (section 2.3.2.), participate in technical standard creation (section 2.3.3), exercise control over the flow of digital information (section 2.3.4) and participate in informal law-making activities. Additionally, individuals who use the system are rights-holders whose rights (including the rights to privacy and freedom of expression, among others) should be protected.

Conclusion

No clear definition or agreed normative framework allows us to identify actors and ascertain who has international legal personality. The debate on subjects of international law reflects the historical origin and development of international law, which has evolved in response to changes in society. The needs of the digital information society have led to the creation of new actors, such as technical standardization entities, who participate alongside business manufacturers in quasi-legal decision-making processes that impact the behaviour of users through their control over the flow of digital information.

The rise of non-State actors has changed society, nationally and internationally, in ways that are increasingly recognized. However, in the absence of an agreed normative approach, efforts to determine the subjects of international law often involve circular reasoning and do not offer concrete solutions. This study adopts a descriptive approach. It identifies all the relevant actors who participate in the digital information ecosystem, in terms of their functions and the actual operation of the information ecosystem. A functional approach is justified because it makes it possible to identify actors in relation to core components of the digital information ecosystem which are necessary for its operation. Core components include: provision of products and services (equipment and devices, software networks, cloud services); using the ecosystem; allocation of resources (such as frequencies and Internet domain names); creation of technical standards used in the different layers of the ecosystem; and creation of laws and non-laws that regulate actors' behaviour. An analysis of activities clearly reveals the extent to which non-State actors, including individuals, have fulfilled functions and contributed to the development of the digital information ecosystem.

Identifying actors of international human rights law does not equate to listing *all* the actors in the ecosystem. To determine which actors have the status of actors in international human rights law, it is proposed to assess the impact of functions on the enjoyment of rights. The main threats to human rights online are associated with the flow of digital information and its life cycle. By examining the capacity of each component of the ecosystem to control the flow of digital information, and identifying the actors responsible for each component, we can discern which components have an impact on human rights and which actors in the ecosystem harm (or protect) human rights. It is proposed that States recognize human rights actors in the ecosystem that have the capacity to threaten (or promote) enjoyment of human rights and establish safeguards to make sure that those actors respect human rights standards.

If an actor in the digital ecosystem acquires the status a human rights actor because it fulfils certain functions, this does not necessarily imply that it has legitimate authority to carry out those functions. Several questions and concerns arise with regard to the legitimacy of human rights actors that *de facto* exercise critical functions in the digital information ecosystem. To resolve issues of legitimacy, it is suggested that States should recognize human rights actors in the digital information ecosystem as actors having obligations under international human rights law. It is also suggested that human rights actors in the digital information ecosystem must themselves claim and implement their human rights obligations so that they can carry out their functions avoiding central regulation. Their legitimacy, as well as the sustainability of the ecosystem, depends on this.

The dynamic nature of the digital information ecosystem and the way it has evolved with little State involvement has created a new typology of human rights actors. These actors are trans-governmental institutions composed of: public authorities (such as regulatory authorities) that are part of government but do not necessarily have the authority to make law; international (Internet) institutions that have evolved organically to resolve problems and whose aim is to expand the Internet; international agencies (established by international organizations) and multi-stakeholder platforms; and industry associations with the status of NGOs. States should recognize these entities as human rights actors; individual rights holders should be aware of these new human rights actors, the functions they fulfil, and the impact of those functions on personal rights.

The digital information ecosystem changes rapidly under the influence of new technologies. The functions that are core to the digital ecosystem both promote and curtail individual rights, by controlling the flow of digital information. As new technologies emerge, they will influence the organization of the digital ecosystem, including the content of its core functions, and may pose new threats to the enjoyment of rights. This means that new human rights actors may also emerge. The core functions of the digital ecosystem are static and stable but they are complicated to understand for people without technical knowledge. By contrast, (human rights) actors in the digital ecosystem are prone to change. For this reason, all human rights actors in the digital information ecosystem need to know who does what in the digital ecosystem, and how their roles are evolving, in order to discern how best to protect human rights. New categories of human rights actors may emerge and all human rights actors, including individual rights holders, need to be aware of the functions they undertake, and the impact of those functions on rights.