# **Submission to the Global Digital Compact**

Submitted by: Ahreum Lee<sup>1</sup>

Note: The current submission is an extract of the author's PhD thesis on "International human rights law in digital space: an examination of the need for new legal measures for the protection of rights online" (PhD in international law obtained in 2020 at the Graduate Institute of International and Development Studies in Geneva, Switzerland). Full version of the thesis is available online.

### 1. The need for reinterpretation and reimagining human rights in digital space

- Against the background of the increased usage of ICTs and its impact on the way humans interact with one another, this Study examined whether we need a new set of norms or additional legal measures to protect the rights of individuals in relation to their activities online. The analysis on the need for new legal measures called for examining whether existing measures both international human rights law and other legal measures sufficiently address the changes in the nature of the impact and whether existing human rights principles and concepts require new interpretation.
- 2. Similar to other existing studies addressing digital rights, this Study also had first embarked the initial research on the widely discussed issues surrounding the right to freedom of expression online and the right to privacy. Indeed, those issues are at the heart of protecting rights online; however, throughout the research, it became clear that the two rights cannot be assessed alone and that other interlinked rights needed to be examined together. Particularly, by examining existing studies, it was noted that the focus on the result of the impact that ICTs has on human beings led to an incomplete analysis as it overlooks the origin and the process that cause those impact (section 2.2.2). To address this point, this Study proposed a human rights-based approach to the digital space as a framework to complement existing studies, taking into account the interdependent and interlinked nature of technologies and that of human rights (section 2.3).

#### 2. Attributes of the digital space and human rights

3. The Study illustrated several complications associated with the protection of human rights in the digital space, starting from the observation that for an individual to enjoy freedom in the digital space, the constraints that need to be removed are different from those of the offline environment (section 7.1.2), the lack of a State's control of activities beyond borders (section 5.3.4), to the complexity observed when information is stored, amalgamated and used (sections 5.3.2 and 5.3.3). These complications are closely related to and derived from the distinct features of digital information and its ecosystem which are the two main attributes of the digital space that impact the protection of human rights. They are: first, the need to embrace the expanded role of digital information beyond the widely recognized concept as a piece of knowledge and second, the specific features of the enabling environment that facilities digital information, namely, the dual functions of its components (section 10.1). These attributes provide guidance to reinterpreting international human rights law in the context of the digital

<sup>&</sup>lt;sup>1</sup> Ahreum Lee is a Human Rights Officer at the United Nations Office of the High Commissioner for Human Rights. The views expressed herein are those of the author and do not necessarily reflect the views of the United Nations. The author can be contacted at: ahreum.lee@un.org

space and lead to the conclusion that we need to contextualize the principles of human rights law that we apply.

## 2.1. Digital information, more than information

- 4. Simply put, digital information is a piece of information in digital form. Based on this primary definition of digital information, Chapters 3 to 6 introduced related concepts found in the international human rights treaties, which are related to conveying facts, description, expression, or other messages and how those concepts remain equally applicable when it comes to new communication technologies. Particularly when the term, "all kind of media", found in article 19 of the International Covenant on Civil and Political Rights (ICCPR) on freedom of expression and its counterpart provisions, is interpreted broadly to encompass innovative developments of ICTs, the digital form of information poses no barrier for protecting rights associated with information such as freedom of expression and access to information.
- 5. In addition to its function as a piece of knowledge, digital information constitutes a means to distribute knowledge and it also constitutes the environment that the means rely on. Digital information is used as a tool to execute actions online and it is also the structure of the system in which it operates. Moreover, digital information represents the identity of individuals online and what individuals actually do online (section 7.1.2.2). Therefore, the rights exercised online are realized by using digital information and the freedom enjoyed online is facilitated by using digital information one way or another. Departing from these broader functions of digital information, this Study focused on the digital format of data, namely, data that can be transmitted through an information system and those that are used as means for individuals to carry out online activities towards realizing and enjoying human rights online.
- 6. In relation to the broader function of digital information, the starting point of this Study was the widely accepted rule that online rights are as equally protected as their offline counterparts, Part II of this Study on human rights in the life cycle of digital information examined whether rights and freedom stipulated in existing human rights treaties are equally extended when those rights are exercised in digital form. The analysis centered on the purposes and functions of actions associated with human rights in the analog environment and how they are equally fulfilled and protected in the digital environment. In doing so, the Study applied the principle of functional equivalence used in electronic commerce law, which states that there is no difference between electronic commerce and brick-and-mortar commerce in terms of their functions and no special treatment is required for electronic communications used in electronic commerce. When applied, the functional equivalent approach identifies certain criteria and conditions for digital communications to be treated as having functional equivalence with that of paper-based communications, for instance, telephone and Voice over Internet Protocol (e.g., Skype).
- 7. However, the recognition of the functional-equivalence of rights online and offline and by extension, the protection offered in the existing human rights framework is not sufficient to answer in the affirmative the question whether the existing legal measures sufficiently address the changes in the nature of the impact on human rights protection brought about ICTs. While there are no legal lacunae that would pose obstacles of a legal nature in implementing existing human rights obligations in the digital space, the current international human rights legal system needs to take into consideration how activities across the stages of the life cycle are inter-linked and how that translates into the interrelatedness of the rights involved. The lack of understanding would pose challenges in maintaining consistency of the implementation of human rights obligations, particularly when it comes to assessing how limitations of rights are justified (Chapter 8).

- 8. The inter-linkage of rights and the magnifying or corollary impact on the restriction of one right on other rights are important aspects that need to be considered when assessing the justification of the measures taken to restrict a right (sections 4.5.1 and 8.3.2). Particularly, the transmission of digital information is not only limited to exercising certain rights, such as the right to freedom of expression, but impacts wider range of other rights. Individuals send, seek and receive digital information in various ways that equate to exercising several rights other than the freedom of expression. As introduced in Chapter 4, the acts of sending and receiving digital information equate to a range of rights from freedom of expression to the rights to assembly and association and to economic, social and cultural rights. It follows that blocking the transmission of digital information from being sent or received constitutes an infringement of other rights. For instance, by disconnecting the access to the Internet, not only does it limit the exercise of freedom of expression but it also limits all rights, which rely on the transmission of digital information through the Internet. Therefore, the limitation needs to be assessed as a whole after having identified impacts from various limitations on rights. Further, the adoption of the functional-equivalent approach should not result in imposing a more stringent standard then that of its counterpart analog method. It would be overly positive to hope that the problem that persists and which is still without a solution in the traditional paper-based world could be solved in the digital world.
- 9. The corollary impacts on other rights are also identified in the disposal stage (Chapter 6). All activities in the digital space are based on digital information and when information is not available or not accessible, all activities online that evolve around the information are limited or cannot be carried out. In turn, the deletion of the content of information or the link to the information in certain situations amounts to a limitation to exercise rights online, particularly those related to receiving digital information and usage stage (section 6.2.2). Therefore, ascertaining the justification of interference with the transmission of digital information should not be limited to freedom of expression or privacy as the transmission involves and implicates the exercise of other rights and should not be limited to those rights (section 6.3.1).

#### 2.2. Digital information ecosystem - "Jekyll and Hyde"

- 10. Digital information and its life cycle rely on a massive system composed of interconnected elements, all of which interact to enable the flow of digital information. Part III focused on this supporting environment what this Study refers to as "digital information ecosystem" (section 2.3.2) and how the access to the layers of ecosystem enables individuals to freely exercise their rights online and at the same time, restrict and limit those rights. Understanding these attributes of the digital information ecosystem is critical to clarify the contents of the human rights obligation of duty-bearers in the digital space.
- 11. For individuals to enjoy freedom in the digital space, the constraints that need to be removed and the safeguards that need to be guaranteed are different from those of the offline environment. Freedom in the digital space requires a new understanding in light of digital technologies and the environment that supports those technologies. As illustrated in Chapter 7, each segment of the digital information ecosystem constitutes an enabling factor for individuals to perform activities online. Specific examples of interferences with rights were illustrated according to the layer of access that constitutes the digital information ecosystem and that form preconditions for ordinary users to conduct any activity online (section 7.1.2.1). These layers are: access to the physical device that allows individuals to create information in digital form and to connect to the digital world; access to the Internet through telecommunication infrastructures; and access to the online platforms where individuals can upload or send digital information; and the access to online contents to receive information in digital format and authorization to read the content.

- 12. These layers are like a coin with two sides: on the one hand, they are necessary enablers of online rights, and on the other hand, by restricting or blocking access to those layers, they lead to interference with or limitation of human rights. For instance, the technical devices, which constitute part of the ecosystem, serve a dual purpose they can restrict access to entire websites, types of online services, specific pages or content within websites or webpages containing specific keywords. Filtering techniques developed initially to shield children from inappropriate content or help businesses block their employees from disclosing confidential information can also be used to block social, religious and political content. The four prerequisite accesses are needed for performing human rights related activities online and can amount to both enablers and limitations for rights online (section 7.1.2). Therefore, one access out of the four, namely the access to the Internet, is not adequate to address the protection of rights online in the digital information ecosystem which is broader than the Internet (section 7.1.1.1).
- 13. The dual functions of digital technology and the digital ecosystem is relevant to international human rights law as it impacts assessment of legitimate restrictions to rights online particularly those involving interception, collection and blocking of digital information. A first example concerns collection and processing of digital information. The reasons for collection can be legitimate in order to fulfill the obligations of certain human rights treaties, for instance, by collecting relevant information about a specific group that may be in vulnerable situations and processing it to disaggregate the information to be used as a basis for establishing a policy (section 5.2.1). However, the same technical act, if used in a different context with a different aim, can amount to negative impacts such as a chilling effect on the exercise of rights online and interference with various aspects of the right to privacy (section 5.2.2). The second example relates to the technique used to rectify data. While the request to rectify data is an act to address the infringement of the right to privacy, the act itself, in a technical sense, is the same as the censorship or blocking of information in certain situation (section 6.2.2).
- 14. Due to the organic way the Internet and its usage have developed, the existing regulatory framework is fragmented with certain regulations covering a specific layer or component of the digital information ecosystem such as the telecommunications industry and content regulation. The digital space is not anarchy and despite different schools of thought on whether the Internet should be regulated (section 7.2.2), the digital space is de facto regulated as there are physical infrastructures (cables, devices and routers) that are bound by traditional telecommunication rules and regulations. Contrast to the concerns put forward that the digital space is functioning separate from the real world, regulation in the online environment is little different to regulation in the real world. Existing human rights norms, particularly those originating from the normative content of certain rights can be adapted to the digital context - these include: availability of infrastructure and services; physical and virtual accessibility; secure and safe access; acceptability; affordability and non-discrimination and net neutrality (section 7.3.1). At the time of writing this Study, it is true that certain aspects of these human rights norms, particularly the availability and affordability of infrastructure and devices, are premature to be recognized as being part of human rights obligations. However, the international human rights law is a framework which accommodates the development of human rights obligations as the role of ICTs find its place in human lives. Section 7.3.2 introduced elements of what constitutes essence of a right in digital space as a way of starting the discussion on those human rights obligations, in other words, whether access to the digital information ecosystem constitutes basic needs and warrants a status of minimum level of access.

## 3. The need for reinterpretation of the right to privacy in digital space

15. The attributes of the digital space that impact the protection of human rights led to the conclusion that we need to contextualize the principles of human rights law that we apply. The main change in nature that impacts the enjoyment and protection of human rights online centers on the protection of the right to privacy in terms of spatial privacy concerning the extent to which private sphere of life are protected for infringement and informational privacy concerning the control over the flow and management of digital information. Moreover, the changes to the nature of risks affect the expectation of privacy protection in the digital space.

#### 3.1. Spatial privacy

- 16. The spatial element of the right to privacy is most prominent at the creation and transmission stage of the life cycle which straddle between the sphere of creator's control in private sphere and outside the individual's control. The first stage of the digital information life cycle deals with created information within the control of the individual both virtually and physically. As a basic requirement, creating digital information involves having access to a device that would allow individuals to create information in the digital form which can be automatically connected to a network (e.g., a mobile phone connected to telecommunication network). Individuals can create digital information by using third-party online services (e.g., email) or by using services that are available offline, without needing to access the Internet (section 3.3.1). Individuals believe that if the information is stored in a device such as a phone in bags or computers in homes, it is within the individual's private sphere. However, the information, which appears to be stored in the devices within your control, is also stored elsewhere on a database outside of the private area of one's control. Most often, there is a copy of information stored in a third party database and thus the third party has access to that information.
- 17. Traditional interpretations of how the two spaces public and private spheres are demarcated do not work in digital space (section 3.3.2). It is not clear whether existing international human rights law covers the way in which digital space creates various combinations where a mix of private and public, as well as workspace, interplay and whether the protection offered under the right to privacy framework sufficiently addresses these combinations. Consider for instance, "quasi-private" spaces where there is a mix of public and private space: these are situations where individuals use personally owned devices and have control over their activities but physically are not in private space, leaving them open for other individuals to observe their online activities. The mixture of spheres created by the interplay of layers of digital information ecosystem lead to legal gaps for the protection of human rights online and hence, a new approach is required for the interpretation and implementation of the protection of privacy in the digital space. This would not call for a new legal instrument but would require a shift in paradigm to understand what is private and what is public in the digital space.
- 18. A proposal is made to define the private sphere as a virtual area where the individual has control over the digital contents that he or she created and has control over how to transmit, store or dispose of this information. The proposed threshold for the distinction is based on the notion of control, identifying the information that is purely within the private sphere and control of the individual as being in private sphere and the information of which the control is shared with a third party, which is the situation at the transmission stage, as being in the public domain. Application of this proposal identifies two points in the flow of digital information that can be considered as the point where the individual relinquishes control over information and control over information from the creator or owner of the digital information shifts to a third party (section 3.3.2.3). The first is the point where the created digital information is stored online in a third-party storage as opposed to in personal digital storage, for instance, saved on a personal laptop. The second point is the point where the individual perceives that the digital information is sent and has left the control of the creator. These two points where the control over

information shifts to a third party as well as those points to be identified along with the development of technology should be taken into account as a standard of protecting rights online.

## 3.2. Informational privacy

- 19. Another recurring discussion is the expansion of the scope of the right to privacy to include informational privacy including the right to request for deletion of personal information. The right to informational privacy is generally understood to mean that individuals as the owners or creators of digital information have the right to know whether and when their digital information is modified or altered. Individuals have the right to control and to be informed of any changes to the flow of digital information. It has been suggested that clarification on the interpretation of the right to privacy is required to explicitly acknowledge informational privacy as being part of the scope of right to privacy, particularly when it comes to control over digital information and storage of digital information by third parties. Chapters 3 to 6 examined whether this blanket approach of simply reinterpreting the right to privacy would be necessary, by breaking down the elements of informational privacy at each stage of the life cycle and checking whether those elements are already covered in the current interpretation and implementation of the right to privacy.
- 20. The notion of informational privacy differs from the perspective of the individual sender who sends information and the individual who passively receives digital information. From the perspective of the recipient, informational privacy concerns the autonomy of the recipient to determine when, how and to what extent others use information about the recipient (section 4.3.3). The act of receiving information can amount to a violation of the right to privacy, in particular, the right to be left alone in the digital space and to live with minimum interference. In the event the digital information is intercepted at one point during transmission, the individual has the right to know when and by whom the interception has been made (section 5.2.3.3). More specifically, the individual involved should be informed of who has accessed his or her data and if this has occurred without their permission, the individual is entitled to know which authority has granted permission or accommodated access and the reasons behind the decision to allow access. The sender, recipient and owner of information should be presented with the information about the process of filtering, blocking and otherwise restricting the flow of information (section 4.4.1).
- 21. These elements of informational privacy are not new to international human rights law. Particularly, when we look at the discussion surrounding the interference with the right to privacy, the UN Human Rights Committee and different judicial mechanisms have interpreted that the storage of personal information and control over that information are covered within the scope of article 17 of the ICCPR on the right to privacy and its counterpart provisions in regional treaties. The collection of personal information or any information produced as a result of individual users' online activities constitutes interference with the right to privacy. In addition to the passive nature of the right to privacy concerning the collection of personal information, the question remains whether individuals have the right to ascertain what happens after their personal information is collected. The right of access to information in connection with article 17 of the ICCPR on the right of privacy implies that individuals have the right to know which personal data is stored and which authorities have access to such data.
- 22. Furthermore, the concepts related to disposal of digital information introduced in Chapter 6 ranging from the right to be forgotten, the right to erasure, among others, are equally not new; they are called with different names but have the common point that all refer to the elements of rectifying information about oneself and the right to dispose of information about oneself, which are found within the realm of the right to privacy. The elements of rectifying or

eliminating digital information constitute corrective measures to address infringement of various aspects of the right to privacy, including personality rights and informational autonomy. The existing international human rights treaties provide a legal framework in which individuals have ways to rectify the infringement of their right to privacy in certain circumstances.

#### 3.3. Expectation of privacy

- 23. Another important change in the nature of impact on human rights is the objective expectation of privacy provided for in the digital information ecosystem. The expectation of privacy in the digital space is closely related to the design and the components of the digital information ecosystem. Depending on the architectural design of the network through which the digital information travels, there are several points within the digital information ecosystem where information may be blocked and censored (section 7.3.1). First, information can be prevented from being sent by certain functions and restrictions embedded in the technological equipment itself. Software that is automatically and mandatorily installed on a laptop or a smartphone prior to purchase may restrict users from dispatching certain text messages by blocking certain country codes or phone numbers in the destination numbers and filtering certain words. At the level of the networks and infrastructure, equipment or computer networking devices such as routers, proxy servers, firewalls, and wireless access points may contain functions to track user activity and store personal information and communication. Security methods, such as network packet filtering, which control what information can flow into and out of the network are some of the examples that provide this functionality. Further, at the level of an online platform, the behaviors of individuals on the site can be monitored and collected in the form of data. The online platform itself, as a space of its own regulation, may have access control schemes where granular access control management is employed to restrict certain individuals to a particular space in that online platform.
- 24. These points within the digital information ecosystem where digital information is blocked interferes with right to privacy during the transmission stage (sections 4.2.4, 4.3.3, and 4.4.1). The change in the nature is related to that fact that the flow of digital information does not follow the territorial boundaries that we know in the physical world and hence, it inevitably results in situations where foreign actors can infringe privacy rights of non-citizens (section 5.3.4). The law would not be able to change how the digital industry functions and how the digital information flows through different routes passing through various territories. Most importantly, a legalistic approach to addressing this issue is probably not effective let alone welcomed by industry players. The role of the law, at least in the digital space, should respond to the changes that market and the people have accepted so that individuals are free to exercise their rights online. This starts with applying current legal measures, for instance, safeguards against risks and abuses developed in surveillance regime cases and existing data protection principles with greater emphasis on durability, veracity, sensitivity and non-rivalrousness of digital information (section 8.4.1).
- 25. Another related change in nature that impacts expectation of privacy is the diversified ways to collect digital information and how these ways can lead to disclosure of unexpected information. The ways of collecting digital information still remains the same as analog collection: get the information directly from the source or from a third party who legitimately or illegitimately has the information or alternatively, eavesdrop and tap into communication means used by the source. In the digital form, these methods of collection translated into voluntary and involuntary collection from the source; collection of information in transit; collection from third-party storage and transfer of collected information (section 5.3.3).
- 26. What is different from the analog collection is the scale of data collected and how the scale impacts disclosure of certain types of information. The current digital space evolves around the

concept of big data which is about predictions and applying math to huge quantities of data in order to infer probabilities, the default norm is to collect as much data as possible so that the samples will reflect reality more accurately. More data is better for "big data" and there is a tendency to collect as much data as possible irrespective of the purpose of the collection (referred to as "blanket interception or collection"). Irrespective of the composition, digital information can unintentionally or at times, intentionally, reveal or disclose private and personal information when collected data is processed. Personal information can be revealed from seemingly insensitive information, and seemingly anonymous data can be linked to explicit information identifying the person associated with the data. Therefore, it is important to understand how the collection and processing of information can lead to a disclosure of personal and sensitive information and subsequently, impact and infringe the right to privacy (section 5.3.2).

#### 4. The need for recognition of new human rights actors in the digital space

- 27. Based on these two analytic frameworks to identify gaps relating to the protection of human rights online (namely, the digital information and digital information ecosystem), the Study focused on whether there was a change in the nature of the impact that digital technologies have on the exercise of human rights online and whether those changes call for new substantive legal measures as opposed to procedural measures. The scope of existing international human rights law composed of treaties and decisions of human rights bodies are sufficiently broad to cover the usage of digital information as a means of exercising rights and as the exercise of rights themselves. However, despite interpreting human rights in the context of the digital space, there still exist gaps and concerns when it comes to the role and responsibility of non-State actors in the digital space, particularly, the power and control that they exercise over the flow of digital information. The State-centric international law, still dominant in the 21<sup>st</sup> century, does not establish clear human rights obligations of actors other than States and hence, there is a need to recognize new human rights actors in the digital space.
- 28. Contextualizing certain principles of international human rights law does not address the human rights protection gaps found in the digital space, namely, that the current international human rights system does not have rules and safeguard to monitor all human rights actors or actors that have functional roles which involve effective control over digital information (section 9.3.2). As argued in Part II of this Study, no substantive changes to human rights protection are required as the existing international human rights law extends to the protection of human rights online. However, the anomaly of existing international human rights law when applied to the digital space is the existence of non-State human rights actors that function as gatekeepers or the master-switch of the digital space exerting control and influence over how individuals exercise and enjoy rights online.
- 29. This Study unfolded the presence and function of non-State human rights actors in the digital space by examining the raison d'être for their existence (section 7.1). As digital information cannot be created or transmitted autonomously, it relies on the ecosystem composed of equipment, devices, infrastructure, and users. The digital information ecosystem that supports online activities is like an onion and the layered nature of its architecture poses a challenge for individuals to understand activities at deeper layers of the Internet that govern the exercise and enjoyment of their rights online. The complicated machinery behind the life cycle of digital information makes the ordinary individual users unaware of who is involved in setting the conditions for the digital information to travel and who has access to that information. For individuals to fully enjoy their rights online, we need to understand who facilitates or impedes the exercise of these rights. Chapter 9 of this Study addressed the question of who are the actors

- that impact human rights online based on the proposed notion of effective control over the flow of digital information.
- 30. There are third-party actors at the backend of the machinery who carry out functions that facilitate digital information and operate and control the ecosystem referred to as the "the invisible hands" (section 4.5.2). Due to their involvement, control over digital information is often shared with third parties that individuals are unaware of and the initial creator or owner of the digital information does not have control over it once it is voluntarily shared or forcefully released. The roles of third party service providers have expanded from assisting communication to actively censoring and limiting the information that is sent and becomes available for the public. Third party service providers can dictate the criteria and requirements for digital information to be intercepted because they have *de facto* access to the digital information. Problems arise as third party entities interpret those limitations in lieu of the judiciary and those private entities have enforcement powers as gatekeepers of the network and the platforms. In the digital space, entities that carry out the role of government in establishing the rule of law online are not only limited to States but can be also business entities or even individuals.
- 31. The dynamic nature of the digital information ecosystem and the way it has evolved with little State involvement created a new typology of human rights actors (section 9.1.2). The needs of the digital information society 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 behavior of users through their control over the flow of digital information. These new types of actors do not fit into the traditional categories of the subjects of international law and hence, international law does not address their human rights obligations and responsibilities. Further, existing types of actors such as business enterprises and individuals are also excluded from the debate on the subjects of international law and are subject to a different legal regime such as the on-going negotiation on a legally binding treaty process for business enterprises. When it comes to individuals as subject of international law, the discussion is limited and the capacity of individuals in the digital space has not yet been considered.
- 32. The Study highlighted that natural persons who use the system or those who provide the products or services that form the ecosystem are also an important element of the digital information ecosystem (section 9.1.3). The Internet is an open architecture with "end-to-end" design allowing anyone to join and develop. In non-technical terms, this means that the original designers of the ecosystem embraced a design that opted for decentralized control of the ecosystem where the end-users have control of how they interact with the ecosystem. This feature of the digital technologies enables individual users to do many things without the assistance of government or businesses. Individuals can be involved in operating critical functions of the digital ecosystem and individuals are also a part of the invisible hands behind the system.
- 33. Identifying actors in international human rights law does not equate to listing *all* the actors in the ecosystem. To determine which actors in the digital ecosystem are actors with human rights obligation, it is proposed to assess the impact of functions on the enjoyment of rights (section 9.3.2). 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 have the capacity to harm (or protect) human rights. This Study proposed that States recognize human rights actors in the ecosystem that carryout functions which to threaten (or promote) enjoyment of human rights and establish safeguards to make sure that those actors respect human rights standards.

- 34. 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 impacting or promoting the enjoyment of individual rights online. Additionally, by virtue of that control, the same actors are in a position to regulate the behavior 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 implemented internal codes of conduct and procedures, even though the legitimacy of the procedures and those responsible for implementing them have never been made clear. Several questions and concerns arise with regard to the legitimacy of human rights actors that de facto carry out critical functions in the digital ecosystem. 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 behavior of individual users or other actors and whether those norms and rules are legitimate. Such need is even more pertinent as the digital industry has moved towards "semantic web" where machines - semantic search assistances such as Siri on Apple devices - play an important role controlling the selections and personalization of user selectivity.
- 35. The answer lies in States' recognition that those actors with effective control over the flow of digital information have are human rights actors having obligations under international human rights law. States should recognize these entities as human rights actors and individual rights holders should be aware of these new human rights actors, the functions they fulfill, and the impact of those functions on rights. To assist States to recognize this, it is suggested that the international human rights system can as a first step, produce an authoritative guidance on how rights stipulated under existing international human rights treaties are manifested and protected in the context of digital space and require States to report on their human rights obligations in digital space (section 9.3.3).