# Online privacy regulation in a decentralized, unbounded context: Internet Governance and multi-stake-holder initiatives as regulatory mechanisms[1]

## La regulación de la privacidad en Internet en un contexto descentralizado y no consolidado: la gobernanza de Internet y las iniciativas de múltiples partes interesadas como mecanismos reguladores

Hugo Fernando Aguiar Lozano[2]
Pérez, Bustamante & Ponce

**Summary**
The present paper analyzes the right to privacy in the context of the Internet. The multi-stake-holder initiatives are an alternative that has already provided a regulatory structure on various aspects of the Internet, be it security, free flow of information or online privacy. Although there are elements that make it not a total solution, this paper analyzes some reasons why online privacy should be regulated by mechanisms of Internet Governance and by entities that do not respond only to governments or only to private firms. In this work, a general look at this alternative is given, without neglecting other approaches that should be applied to the topic of online privacy.

**Keywords**
Internet Governance/ Right to Privacy/ Online Privacy/ Regulation.

**Resumen**
El presente artículo analiza el derecho a la privacidad en el contexto del Internet. Las iniciativas de múltiples partes interesadas son una alternativa que ya ha proporcionado una estructura regulatoria en varios aspectos de Internet, ya sea la seguridad, el flujo libre de información o la privacidad en línea. Aunque hay elementos que hacen que no sea una solución total, este artículo analiza algunas razones por las cuales la privacidad en línea debe ser regulada por mecanismos de Gobernanza de Internet y por entidades que no responden solo a los gobiernos o solo a empresas privadas. En este trabajo, se da una mirada general a esta alternativa, sin descuidar los otros enfoques que se deben dar al tema de la privacidad en línea.

**Palabras clave**
Gobernanza de Internet/ Derecho a la Privacidad/ Privacidad en línea / Regulación.



## 1. Introduction

The concept of the term "privacy" is complex because it depends on many conditions of all kinds. From the regulatory point of view, and particularly from the legal perspective, it is important to circumscribe the right to privacy as a consideration of rights that must be protected.

There are many ways in which you can try to solve all the problems that arise in

1Recibido: 06/03/2018 – Aceptado: 11/09/2018

2 Abogado por la Pontificia Universidad Católica del Ecuador, mejor egresado de su promoción y graduado de la Escuela de Derecho de Harvard University, además posee varios títulos de posgrado. Tiene experiencia en distintas áreas del Derecho. Ha ejercido cargos diversos en instituciones públicas y privadas. Actualmente es abogado de la firma Pérez, Bustamante & Ponce. Es catedrático universitario y autor de libros y artículos jurídicos.

Hugo Fernando Aguiar Lozano (2018). Online privacy regulation in a decentralized, unbounded context: Internet Governance and multi-stake-holder initiatives as regulatory mechanisms, *Iuris Dictio 22,* 205-216.
ISSN 1390-6402 / e-ISSN 2528-7834.
DOI: http://dx.doi.org/10.18272/iu.v22i22.1063

relation to the right to online privacy. The concept of privacy within a more complex and interconnected context implies the search for solutions from several edges. The natural response to regulation is the one that supposes that governments should legislate or regulate the specific cases or that courts or other organizations of control should fix the limits on the handling of the personal data. On the other hand, a market response is expected in which a self-regulation is required and is driven by market incentives in the conditions set by the industry.

Finally, there is a solution that involves the very structure of the Internet, since this is a decentralized scheme; it is assumed that the setting of standards must be done in an open, transparent and representative manner. The multi-stake-holder initiatives are an alternative that has already provided a regulatory structure on various aspects of the Internet, be it security, free flow of information or online privacy. Although there are elements that make it not a total solution, this paper analyzes some reasons why online privacy should be regulated by mechanisms of Internet Governance and entities that do not respond only to governments or only to private firms. In this work, a general look at this alternative is given, without neglecting other approaches that should be given to the topic of online privacy.

**2. First things first. What is privacy?**

Privacy is a difficult term to define because there are different perspectives from where you can see it. Each discipline, whether law, psychology, sociology, or philosophy has its own definition and its own values overlaying the concept. What is clear is that the term private could first be understood in contraposition with the term public and in this sense the right to privacy is a reaction to the general idea that there should be a free flow of information. "Privacy has an image problem […] Regardless of the forum in which it is debated; it is cast as old-fashioned at best and downright harmful at worst —antiprogressive, overly costly, and inimical to the welfare of the body politic" (Cohen, 2013, p. 1904). It is interesting to understand the values that support the concept of privacy, because in general when privacy is balanced against national security, efficiency and entrepreneurship, privacy never wins. With technology advancing so fast and relentlessly, privacy is in permanent opposition to the progress of knowledge (Cohen, 2013).

It is very difficult to have a consensus in a single definition of the term "privacy", basically because its value depends on the cultural or historical background that every society has for it. That is why its protection comes from law and society in different spectrums. For instance, some may think that privacy is protected incidentally when other interests or rights are protected, for instance, rights to property and bodily security (DeCew, 2015).

When it comes to the American Constitution, in *Roe v. Wade,* Justice Douglas couldn't define the right to privacy, when he pronounced the famous adjective of "penumbral right emanating from the Constitution" (US Supreme Court, 1973). In general, one could understand the Court's intention to define the right to privacy as the right to protect one's individual interest in independence, especially when it comes to making important and personal decisions about one's family, life and lifestyle (DeCew, 2015).

"Privacy is a concept in disarray. Nobody can articulate what it means" (Solove, 2006, p. 70). Because of this conceptualization it is difficult to have a concrete regulation or adjudication on privacy. Besides this specific difficulty, in today's world called the "information age" privacy problems have been amplified in size and in magnitude. For the purposes of this paper this article will not try to dissect the concept of privacy, but it would begin from the base of understanding privacy in contrast with a specific society. Then, sociology could be a useful tool to explain that privacy is a reflex concept or a created need. "Privacy is the relief from a range of kinds of social friction" (Solove, 2006, p. 484).

In a very general way, we can see privacy as an umbrella term. It seems interesting how Solove tries to create taxonomy of privacy in the sense that there should be at least various groups of situations where privacy related issues could be categorized and then studied and, in the long term, some policy recommendations could be done to solve those issues. In his proposed taxonomy, Solove presents four groups of harmful activities that directly affect privacy. "(1) Information collection, (2) information processing, (3) information dissemination, and (4) invasion" (2006, p. 488). We part from the idea that an individual is in risk when other individual, businesses or the government can inflict harm through an activity. The harm is measured after the infliction of a particular activity that by itself is not good or bad.

As we can see, the activities that affect privacy are "not necessarily socially undesirable or worthy of sanction or prohibition" (2006, p. 559), and that is precisely what makes privacy so difficult to handle. This paper considers the concept of the role privacy in relation to the legal system which understands privacy as "a form of protection against certain harmful or problematic activities" (2006, p. 559). In the context of a comparative online privacy methodology this conception will be important when applied to specific scenarios such as big data or the Internet of Things, particularly when understood under the activities of surveillance, data collection and data processing.

## 3. The complexity of the battleground

Information, knowledge, and information-rich goods and tools play a significant role in today's economic opportunity and human development, but they play a more interesting one when we want to protect people's privacy as well. It seems that since information in general has gained more value in our society, privacy as well is regarded as more valuable for the dangers of being affected by innovation. When we talk about online privacy we must contemplate the complete picture and how privacy works in the online setting (Benkler, 2006, p. 13).

The Internet opened a myriad of opportunities that could not have been envisioned before and currently, we live in a society where it is almost impossible to escape from digital technology. "While the networked information economy cannot solve global hunger and disease, its emergence does open reasonably well-defined new avenues for addressing and constructing some of the basic requirements of justice and human development" (p. 13) Nevertheless, the emergence of networked information economy has brought some other concerns as well, and one of those are: privacy and security. In fact, "digital privacy has been a hot topic since the Internet became a popular medium in the mid-1990s. Never before has as much information about average citizens been so easily accessible to so many" (Palfrey and Gasser, 2008, p. 53).

The Internet could be conceived as a complex electronic communications network or a network of networks which connects computer networks and organizational computer facilities around the world (Rouse, 2016). One particular concern is how to ensure governance over new technologies, or how to shape, regulate, and control their use. Whereas the industrial revolution generated large-scale technologies whose control required centralized decision-making by national authorities, "the information revolution has produced global technologies whose control resides largely in the hands of individuals. The obstacles to governing such technologies are tremendous" (RAND Corporation, 2000).

Vint Cerf, one of the creators of Arpanet, the precursor of today's Internet, when asked by Esquire magazine: "Will we shoot virtually at each other over the Internet?", he responded: "Probably not. On the other hand, there may be wars fought *about* the Internet?" (Esquire, 2008). Certainly, at this point of history, some countries' leaders are raising their voices of concern over the Internet control and regulation.

Former Brazilian president Rouseff, in the year 2013 took the podium at the UN's General Assembly to call on other countries "to disconnect from US Internet hegemony and develop their own sovereign Internet and governance structures" (Meinrath, 2013). In fact, the misbehavior of American's National Security Agency caused other countries to want to fight back stewardship of the web away from the US[3]. But Rouseff´s move raised concerns about the probability of a powerful backlash against an open Internet, "one that would transform if from global commons to a fractured patchwork severely limited by the political boundaries on a map" (2013). "It is the end of the Internet" (Grassegger, 2014) was the headline of one of the prominent Swiss newspaper. As a response to this trend, Tim Berners, another father of the Internet, called for a "re-decentralization" of the Internet. "I want a Web that's open, works internationally, works as wells as possible, and is not nation-based" (Maurer and Morgus, 2014).

**4. Multi-stake-holder initiatives and online privacy**

There's a growing concern over the "balkanization" of the Internet and the emergence of "splinternets"[4]. The explanation of the term "Internet balkanization" is a modern metaphor for the geopolitical process that took place in the Balkan Peninsula in the context of the Ottoman Empire, leading to the fragmentation of the region in smaller non-cooperative states (Alves, 2014, p. 1). Two possible threats to the Internet, caused by this balkanization, are: structural censorship and the loss of net neutrality. This means that the Internet might break apart along nation-state or commercial boundaries. Some people believe that this might be a technical matter; however, politics play a key role.

We must remember that Edward Snowden's revelations about the United States spying on various world leaders and its own citizens, was the reason for voices trying to introduce the idea of Internet's balkanization in the public domain. In any case, by now, states are passing national laws requiring data pertaining to their citizens to be stored locally instead of shipped around the Internet. There is a trend in raising barriers to the free flow of information based on privacy and cybersecurity issues (London School of Economics, 2014).

One question is if we can have both privacy and security in the Internet time or not. The big challenge is how to ensure privacy protection while assuring national security. It seems impossible to be secure without giving up some privacy. "There's also the increasing complexity of cross-border terrorism and asymmetric war, and the full-on return of interstate strategic conflict. Thus, keeping distinctions between domestic and international does not work anymore" (Kaspersen, 2015).

Government agencies can collect every bit of information that we produce as individuals, what is known as our digital footprint, metadata, online habits and digital history. That works too for businesses and it appears to be a partnership between governments and businesses to collect, processes and analyze all that data. For instance, there is this fear of having smart TVs recording our private conversations. US consumer rights organization the Electronic Privacy Information Center (Epic) accused Samsung of breaking federal privacy laws including the Electronic Communications Privacy Act and the Children's Online Privacy Protection Act, which both concern the collection and disclosure of electronic communications (Gibbs, 2015).

3 "Rouseff's plan to create walled-off, national Intranets followed reports that the United States has been surveilling Rouseff's email, intercepting internal government communications, and spying on the country's national oil company, so it was somewhat understandable" (Meinrath, 2013).

4 "Networks that are walled off from the rest of the Web" (Maurer y Morgus, 2014).

In this scenario, the first question that comes to mind is: do we need a global internet legal framework that protects the open and unrestricted Internet while not compromising the right to privacy? The first reaction could be a no, but the answer is not a simple one. Internet governance is much more complicated because the Internet is not administered by a centralized authority. Internet Governance presents quite a challenge as the Internet simply does not care about traditional borders. We also, should be aware that authoritarian regimes are wary of losing their grip on power due to the Internet, and they desperately are seeking to regain it by imposing new rules and regulations (Schaake, 2016).

"When we think of the Internet, we likely imagine a sprawling network of computers circling the globe, blasting information to each other 24 hours a day" (Love, 2013). The Internet is a "living" thing. Unlike inventions such as the lightbulb, the Internet does not have a single inventor; instead it has evolved over time (A&E Television Networks, 2016). In 1974 we had the Arpanet and it has evolved to what we have today. The Internet has changed the way we work, socialize, create and share information. Additionally, the Internet is transforming the way we organize the flow of ideas and things.

"The change brought about by the networked information environment is deep. It is structural. It goes to the very foundations of how liberal markets and liberal democracies have coevolved for almost two centuries" (Benkler, 2006, p. 1). On the other hand,

> as the world becomes more digital, the importance of understanding threats in cyberspace cannot be overstated. The common response from decision-makers has been to enact legislation and institute regulations, but these efforts have been largely reactive and uninformed, evidenced by their failure to mitigate the evolution of cyber threats (Kaspersen, 2015).

From 2006 until 2011 the Internet accounted for 21 percent of the GDP growth in mature economies (Manyka and Roxburgh, 2011, p. 1). According to a Pew Research Center survey, by the year 2014, 87% of American adults used the Internet up from 14% in 1995 (A&E Television Networks, 2016). The World Bank estimates that, worldwide, 44 people out of 100 are using the Internet while back in 1995 just one out of 100 people worldwide used the Internet (2016). We are beginning to experience the real transformations the Internet has brought about, and we still expect many technological innovations to emerge. However, we must also think of the threats to Internet access and must look for implementing principles of freedom of expression and the free flow of ideas over the Internet (Nye, 2014, p. 4). As Leslie Daigle, the first woman to become selected to lead the Internet Architecture Board puts it: "The biggest challenges are things that tear the Internet into islands: internationalization, middle boxes, and the advent of small devices. It is about stripping down and getting back to the basics" (Marsan, 2015).

We must acknowledge that the Internet is the first modern communications technology that expands its reach by decentralizing the capital structure of production and distribution of information, culture and knowledge. This characteristic of the Internet means that "much of the physical capital that embeds most of the intelligence in the network is widely diffused and owned by end users" (Benkler, 2006, p. 30).

In this context, the Internet has a peculiar governance structure. This comes from its own nature, which is a decentralized, distributed network that is based in voluntarist, non-coercive, non-hierarchical and open design. The Internet is complex and therefore its governance is not entirely clear. Internet Governance as far as we know is "the application by governments, the private sector and civil society of principles, norms, rules, procedures and programs that shape the evolution and use of the Internet" (WGIG, 2005, p. 4).

One of the first models of governance of the Internet is known as the Internet Engineering Task Force —IETF—, which was designed so there is no top node, with no formal accreditation, with a lack of formal power, however it proved to be successful in guiding the behavior of internet users and setting standards or norms for action (Benkler, 2013, p. 217). In words of Benkler, "it is interesting that this model governed a public good, the Internet, that is the most important new global infrastructure" (p. 218). We must acknowledge that the current multi-stakeholder initiative —MSI— is the most flexible governance model to balance interests and settle disputes. There is much potential on MSIs that could be catalyzed if there are enough resources to start a global campaign directed to build capacity and institutionalize MSI[5].

On the other hand, we should also keep in mind what Joseph Nye argues when he says that even though the Internet has been portrayed as the end of government controls "in practice, governments and geographical jurisdictions have been playing major roles in cyber governance right from the start" (Nye, 2014, p. 5). For instance, governments control copyright and intellectual property laws, privacy laws, and they determine national spectrum allocation within the framework negotiated at the International Telecommunications Union—ITU—.

Recognizing the key role of all stakeholders in Internet Governance, i.e., governments, the private sector and civil society, as well as intergovernmental and international organizations is essential, in order to improve the criteria of the MSIs for transparency, accountability, legitimacy, multilateralism and the need to address all public policy issues in a voluntary, consensus decision-making model. In Laura DeNardis' words: "a question such as 'Who should control the Internet, the United Nations or some other organization?' makes no sense whatsoever. The appropriate question involves determining what the most effective form of governance is, in each specific context" (Nye, 2014, p. 7).

We must be clear about Internet's governance structure. On one hand, access to the Internet has so far been relatively open and unrestricted. On the other hand, organically, a governing system has developed in which business, organizations, governments and users all play their part. It is basically a MSI and it seems to give a decision power and influence of all stakeholders. We also must say that multilateral organizations are pushing back in trying to become important arenas in the Internet Governance. This attempt has failed so far. For instance, at the UN level the Internet Governance Forum, which co-exists with the ITU, has been the forum for the proposition of the balkanization of the Internet but this attempt has been unsuccessful. On the other hand, the right to privacy has brought up more attention from the United Nations General Assembly specifically related to the pervasive impact that surveillance and interception of communications have on human rights. "The General Assembly affirmed that the rights held by people offline must also be protected online" (The Human Rights Council, 2018, p. 18).

China, Russia, Brazil, India, and Turkey, and even some countries in the European Union among other countries have tried to set an agenda in order to gain control over the Internet with poor results. However, authoritarian regimes such as China and Russia are gaining ground by influencing developing countries to vote in favor of their proposals that

5 MSI could be defined as a form of governance, a structure that brings stakeholders together to participate in the dialogue, decision making, and implementation of solutions to common problems goals. In other words, "we can identify these multi-stakeholder initiatives as initiatives governing social and/or environmental standards of production that have participants from both business and societal interest groups as members and governance structures allowing for an equal possibility of input among the different partners in steering the initiative" (Fransen, 2012, p. 166).

aim for a centralized control of the Internet. They have framed their agenda as a fight on cybercrime; therefore, they propose to regulate information services. It is in these forums that governments and businesses are waging an ongoing battle to regain influence and power online (Schaake, 2016).

Additionally, net neutrality concerns are into play. Simply put, net neutrality means that Internet Service Providers —ISPs— cannot discriminate online and create pay-to-play fast lanes (Freepress, 2016). This is more a pushback of ISPs that seeks to profit from their monopolistic power over the Internet backbone structure. ISPs want to transfer costs to end-users. Net neutrality keeps Internet open and free and if ISPs are allowed to discriminate online, the whole concept of the Internet will change and could bring unexpected consequences in terms of affecting user's rights online. For instance, startups could end up paying massive amounts of money when their service suddenly becomes a success. As we have seen so far attempts from Comcast to charge Netflix a different rate because of the increasing success of their video streaming service has been stopped by the US Government due to the intense pressure applied by other big information companies such as Google and Amazon (Lynley, 2018).

We must add the importance of the economic and social benefits that the Internet has brought has been possible, in great account, because of the lack of an Internet bureaucracy and a strict regulatory framework. The vision of the Internet as a major source of innovation and creativity is best preserved by keeping the Internet open and by protecting its users (Schaake, 2016).

The idea that the Internet democratizes is not new, however the strength of its democratizing power has been recently noticed by authoritarian regimes who are struggling to stop innovations and information free flow. Let us remember, for instance the relatively simple first-generation claims about the liberating effects of the Internet, expressed in the US Supreme Court's celebration of its potential to make everyone a pamphleteer, and later came under a variety of criticisms and attacks. There is no doubt that "the emergence of a networked information economy as an alternative to mass media, improves the political public sphere" (Benkler, 2006, p.10). And because of this same reason "no benevolent historical force will inexorably lead this technological-economic moment to develop toward an open, diverse, liberal equilibrium" (p. 22).

> In order to keep the Internet open and unrestricted for all of its users worldwide it is imperative to prevent governments from taking the initiative to restrict the Internet or from creating normative barriers. We must foment and build capacity in the multi-stakeholder initiatives. Additionally, active participation of Internet's users around the globe is essential and should be promoted. Users should feel that they have a voice and can influence to keep the internet open (p. 29).

It is clear that governments and corporations opposing the free and open Internet have framed their stance as a reaction to cybersecurity. They claim that the US government is taking over the Internet and therefore they instill fear on other countries. They have noticed that having a "common enemy" is the easiest way to channel all the efforts to regulate the Internet. By using fear, they have framed the Internet as a dangerous, powerful and uncontrolled tool. The supporters of the balkanization of the Internet are managing to influence countries by telling them that the Internet is a means that destabilizes institutions and creates risks in government structures and even in market structures. They have used the Snowden's disclosures as a trampoline to spread their ideas. They have managed to frame "the Snowden effect" so as to

increase public concern about information security and privacy. They have framed the idea that not just governments, but tech companies as well are "spying" everyone. The Snowden leaks ignited a crisis of confidence and conscience throughout public opinion (Gunaratna, 2016).

During the 1970s and early 1980s some European countries raised some concerns about "data sovereignty", the reason was that the United States' hegemony was already emerging in cross-border data services. There was a growing fear of increasing quantities of sensitive personal data about their nationals being stored in a foreign country.

> Since then, a key stated objective of almost all international initiatives to promote harmonization of data privacy rules has been to facilitate the free movement of personal data between states that make a commitment to enforce certain, more or less, basic, data protection principles (Kruner, 2015, p.1).

Strong privacy protection is critical to ensuring that the Internet fulfills its social and economic potential. Therefore, privacy rules should be based on globally recognized principles, such as the OECD privacy guidelines, and governments should work to achieve global interoperability by extending mutual recognition of laws that achieve the same objectives […] Privacy rules should also consider the fundamental rights of others in society including rights to freedom of speech, freedom of the press, and an open and transparent government (OECD). Everyone has a right to the protection of personal data and private life on the Internet and other ICTs -information and communications technologies-. Users should be protected against the unlawful storage, abuse or unauthorized disclosure of personal data, and against the intrusion of their privacy (UNESCO). Efforts should be made, in conjunction with all stakeholders, to create arrangements and procedures between national law enforcement agencies consistent with the appropriate protection of privacy, personal data and other human rights (WSIS) (Cooper, 2013, p. 90).

The Obama Administration released, in 2012, a White Paper denominated "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy". This paper has a proposal on a Consumer Privacy Bill of Rights which introduces some of the fair information principles with the idea of helping shape a future federal law. The idea of the Obama Administration was to stablish high standards but to delegate this practice to multi-stake-holder negotiations, but specifically to market-driven responses to privacy. "Internet technical standard setting bodies are one possible vehicle for multistakeholder activities to address privacy concerns under the Administration's initiative" (Dotty and Mulligan, 2013, p. 136).

"Proponents of multistakeholder processes, including the US government, suggest that this mode of policymaking benefits from important advantages, including an opportunity to coopt industry experts, move swiftly to conclusion, and garner industry support" (Tene and Hughes, 2014, p. 438). For example, the World Wide Web Consortium (W3C) proposed what they called the "Do Not Track (DNT) standard". In fact, the Tracking Protection Working Group looks forward to improving users' privacy and user control by controlling user's mechanisms to be able to express their preferences related to Web tracking and for blocking or allowing Web Tracking systems (World Wide Web Consortium , 2013). This standard proposal was controversial because it represented a "black or white" approach or an "on-off" approach to data collection and privacy.

On the other hand, some concerns came about self-regulating attempts by the industry itself. Some argued that this approach was an easy way-out to formal regulation.

In general, we can see various cases were self-regulation failed in the area of privacy. For instance, according to a study performed to 361 consumer-oriented commercial Web sites by the Georgetown Internet Privacy Policy it reaches the conclusion that self-regulatory regime for consumer privacy online has yet to emerge (Mary and Culnan, 2000). But in fact, there is a complex relationship between markets and privacy, as well as the relationship between government and privacy. One big problem related to privacy is information asymmetry between people and both government and the industry. From an economic perspective privacy is "overrated, inefficient, and perhaps even immoral […] Privacy hides information and in so doing compromises market optimization" (Calo, 2015, p. 652).

However, one can assume that privacy is not always inefficient and that there is a market for privacy hence arguing that privacy is the new business model. "Trust is a new type of capital. The personal data of users has frown the dawn of the internet era been the heaviest currency in the digital media business model, easy to quantify and to transform into a profitable trade" (Lapenta, 2013). This perspective sees at privacy not just as a legal obligation but as business innovation opportunity. As people get savvier and more aware of the importance of security of their personal data, there will be a push for business to comply with people expectations. As an example of this approach, Apple sees privacy as a competitive advantage over Google, because for Apple their "core revenue stream is not tied to monetizing data" (Balkan, 2015). Even though people's concern over privacy can create market-based solutions and bring new business models, it probably will be marginal and will depend on people's capacity to outweigh their preferences between the price they pay for a service or product versus the value they give to their personal data. A Pew Research Center study found that "most Americans see privacy issues in commercial settings as contingent and context-dependent" (Rainie and Duggan, 2016).

Policy-making is a mined field; more so in the realm of privacy regulation. Whether in the United States or Europe the debate over privacy regulation goes beyond its merits, format and contents of privacy legislation. Perhaps the only area of coincidence is that privacy law requires a reform. Even the most basic concepts have not been settled. For instance, "personally identifiable information, the most basic building block of an information privacy framework, remains one of the most contentious concepts in privacy, igniting frequent disputes between engineers and lawyers involving science, philosophy, and a healthy dosage of political spin" (Tene and Hughes, 2014, p. 441). Therefore, it is unlikely to create a consensus in privacy regulation in the next years. Technological innovation is advancing faster than regulation or policy-making processes. In today's world of big data evolution and interconnected smart devices gathering information in every possible location a government only-solution or a private sector only-solution seem inviable.

"A multi-stake-holder approach to privacy responds to a perceived weakness of the traditional 'command-and-control' regulation over the internet" (Dotty and Mulligan, 2013, p. 139). Hence, in order to face the internet's policy issues on the global stage, civil society organizations have an important role to play. There are potential risks related to rights and freedoms that come from governments or the industry. Therefore, a stronger MSI system must be implemented to guarantee transparency in decision-making and in regulation of standards at least in some areas. Legitimacy is another aspect that can be guaranteed trough a MSI. If in fact an MSI is not the solution to all issues generated by privacy concerns over the internet, at least is a great alternative that goes beyond borders and does not depends directly to specific countries' sporadic political state of affairs.

## 5. Conclusions

It is evident that at present, many things that were considered private are no longer so. All our activities as well as our everyday communications leave traces of information through devices or networks. This information can be collected, monitored, processed and analyzed in many ways. There is still a lack of awareness about the exposure we face in our daily activities. But it is not only the problem of the raw data that we leave but, in the inferences, and the manipulation that we can be object on the part of the corporations or governments. This misuse that can be given to our information remains one of the most dangerous aspects to be corrected. The vulnerability of being exposed to any kind of personal injury is a direct effect of the lack of adequate regulation.

Regulation and policy in relation to online privacy cannot be generated spontaneously, but it must be delineated by the different forces in every society or under each cultural lens. The future flow of ideas generated by the conflicts of interest of the various groups involved in this complex scenario will delineate the global shape of online privacy. The truth is that we cannot escape a reality, and we are not fully prepared to face all the technological changes that are coming. Human behavior is still very sensitive to uncertainty. While the real effects of the threats to privacy in our society or in our psychology are deciphered, the financial or monetary cost will be the spearhead to generate the necessary checks and balances in the regulatory framework that will allow the free flow of information with the greater confidentiality possible and above all respecting the private and sensitive data. "To be effective, privacy policy should protect real people –who are naïve, uncertain, and vulnerable- and should be sufficiently flexible to evolve with the emerging unpredictable complexities of the information age" (Aquisti and Brandimarte, 2015, p. 514).

"Bringing privacy concerns into the design of technical standards and ultimately products that rely on them, offers an opportunity to quell the struggle, or at the very least understand and contain it" (Dotty and Mulligan, 2013, p. 180). This kind of approaches could have their base at the multi-stake-holder initiatives that form the Internet Governance and respond to the structure of a highly networked society. Spaces created to deal with privacy concerns, such as the W3C, can generate the necessary technical expertise to face the modern privacy needs. Even though all these attempts should be tested in real life situations, and further study should still be performed, MSIs are another road to regulate, set standards and generate the necessary regulation to comply with the basic principles of online privacy.

## Bibliographic references

Alves, S. (2014). Internet Governance: The Internet Balkanization Fragmentation. Draft *20th ITS Biennial Conference*, 1-15.

Aquisti, A. and Brandimarte, L. (2015). Privacy and human behavior in the age of information. *Science*, 30, 509-514.

Benkler, Y. (2013). Practical Anarchism: Peer Mutualism, Market Power, and the Fallible State. *Politics and Society*, 41 (2), 213-215.

Benkler, Y. (2006). *The Welth of Networks.* New Haven and London: Yale University Press.

Calo, R. (2015). Privacy and Markets: A Love Story. *Notre Dame Law Review,* 91, 649-690.

Cohen, J. (2013). What Privacy is for. *Harvard Law Review*, 126, 649-690.

Cooper, M. (2013). Why growing up is hard to do: institutional challenges for internet governance in the "quarter-life crisis" of the digital revolution. *Journal on Telecommunications & High Technology Law* 11 (1), 45-113.

DeCew, J. (2015). Privacy. *The Stanford Encyclopedia of Philosophy*. <https://plato.stanford.edu/archives/spr2015/entries/privacy/>.

Dotty, N. and Mulligan, D. (2013). Internet Multistakeholder processes and Techno-Policy Standards: Initial Reflections on Privacy at the World Wide Web Consortium. *Journal on Telecommunications and High Technology Law*, 11 (1), 135-184.

Fransen, L. (2012, January). Multi-Stakeholder Governance and Voluntary Programme Interactions: Legitimation Politics in the Institutional Design of Corporate Social Responsibility. *Socio-Economic Review*, 10 (1) (1), 163-192.

Kruner, C., Cate, F., Millard, C. and Svantesson, D. (2015). Editorial: Internet Balkanization gathers pace: is privacy the real driver? *International Data Privacy Law* 5 (1), 1-2.

Lapenta G. H. (2013). Background paper, Privacy as Innovation III. < https://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/background_paper_Privacy_as_Innovation_III.pdf >

Manyka, J. and Roxburgh, C. (2001). *The great transformer: The impact of the Internet on economic growth and prosperity.* San Francisco: McKinsey Global Institute.

Mary, C. and Culnan, M. J. (2000). Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy & Marketing ,* 19 (1), 20-26.

Nye, J. S. (2014). The Regime Complex for Managing Global Cyber Activities (pp. 4-20). *Global Commission on the Internet Governance*. London: CIGI.

Palfrey, J. and Gasser, U. (2008). *Born digital: understanding the first generation of digital natives.* New York: Basic Books.

Rainie, L. and Duggan, M. (2016). Privacy and Information Sharing. *Pew Research Center* (Dec.), 1-45.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review,* 154, 477-570.

Tene, O. and Hughes, T. (2014). The Promise and Shortcomings of Privacy Multistakeholder Policymaking: a Case Study. *Maine Law Review* , 437-465.

The Human Rights Council. (2018). *Report of the Special Rapporteur on the right to privacy.* <https://www.ohchr.org/en/hrbodies/hrc/.../a_hrc_37_62_en.docx>

The London School of Economics and Political Science (2014). Unfield Field: The "Splinternet". *Media Policy Project Blog*. <http://blogs.lse.ac.uk/mediapolicyproject/2013/11/18/unified-field-the-splinternet/>

The World Bank Group. (2016). Internet users per 100 people. *The World Bank Indicators*. <http://data.worldbank.org/indicator/IT.NET.USER.P2>

WGIG. (2005). *Report of the Working Group on Internet Governance.* Chateau de Bossey. <https://www.wgig.org/docs/WGIGREPORT.pdf>

World Wide Web Consortium (2013). Tracking Protection Working Group. *W3C*. <https://www.w3.org/2011/tracking-protection/>

**Articles and News**

A&E Television Networks. (2016). The Invention of the Internet. *History*. http://www.history.com/topics/inventions/invention-of-the-internet

Balkan, A. (2015). Apple vs Google on privacy: a tale of absolute competitive advantage. https://ar.al/notes/apple-vs-google-on-privacy-a-tale-of-absolute-competitive-advantage/

Esquire. (2008). Vint Cerf: What I've Learned. *Esquire Entertainment Interviews*. http://www.esquire.com/entertainment/interviews/a4451/vint-cerf-0508/

Freepress. (2016). Net Neutrality: What you need to know now, *Free Press Action Fund*. <http://www.savetheinternet.com/net-neutrality-what-you-need-know-now>

Gibbs, S. (2015). Samsung's voice-recording smart TVs breach privacy law, campaigners clalim. *The Guardian*. <https://www.theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim>

Grassegger, H. (2014, February 9). States are emerging from the Web. *NZZ Mediengruppe*. <http://www.nzz.ch/nzzas/nzz-am-sonntag/das-ende-des-internets-1.18239023>

Gunaratna, S. (2016). The Snowden effect: Silicon Valley vs. the government. *CBS NEWS*. <http://www.cbsnews.com/news/the-snowden-leaks-effect-its-now-silicon-valley-vs-the-government-privacy/>

Hasselbalch Lapenta, G. (2013). Privacy is the new business model. *Mediamocracy*. <https://mediamocracy.files.wordpress.com/2013/08/download-the-article-in-pdf-here.pdf>

Kaspersen, A. (2015, July 21). Can you have both security and privacy in the internet age? *World Economic Forum Global Governance*. <https://www.weforum.org/agenda/2015/07/can-you-have-both-security-and-privacy-in-the-internet-age/>

Love, D. (2013, June 29). Business Insider. *Tech Insider*: <http://www.businessinsider.com/10-crazy-facts-from-internet-history-2013-6>

Lynley, M. (2018, April 13). *Techcrunch*. <https://techcrunch.com/2018/04/13/comcast-will-start-bundling-netflix-into-its-cable-subscriptions/>

Marsan, C. (2015). "New IAB chair fears Internet balkanization", *Network World*. <http://web.archive.org/web/20080404025305/>

Maurer, T. and Morgus, R. (2014, February 19). *Slate*. Retrieved December 3, 2016, from Stop Calling Decentralization fot he Internet "Balkanization". <http://www.slate.com/blogs/future_tense/2014/02/19/stop_calling_decentralization_of_the_internet_balkanization.html>

Meinrath, S. (2013, October 11). The Future of the Internet: Balkanization and Borders. *Time.* http://ideas.time.com/2013/10/11/thefutureoftheinternetbalkanizationandborders/

Pew Research Center (2016). Number, Facts and Trends Shaping your World. <http://www.pewinternet.org/data-trend/internet-use/internet-use-over-time/>

RAND Corporation. (2000). Where Will the Information Revolution Lead? *Transcendental Destination.* <http://www.rand.org/pubs/periodicals/rand-review/issues/rr-12-00/transcendental.html>

Rouse, M. (2016). Internet technologies. *Tech Target*. <http://searchwindevelopment.techtarget.com/definition/Internet>

Schaake, M. (2016). The World Post. *The Huffington Post*. <http://www.huffingtonpost.com/marietje-schaake/stop-balkanizing-the-internet_b_1661164.html>

**Sentences**

U.S Supreme Court (1973). *Roe v Wade 410 US 1*13. Jan. 22, 1973.