dos Santos, J Comput Sci Syst Biol 2018, 11:3
DOI: 10.4172/jcsb.1000273

Journal of
Computer Science & Systems Biology

Review Article Open Access

They See you and yet you Don´t See them: Privacy in the Multilayered National Surveillance State Realm: A Dystopian Digital Society?

Hugo Luz dos Santos*

Magistrate Public Prosecutor (Portugal), International Legal Advisor, 聯邦大廈749號R/C, Macau, China

Abstract

The concept of digital society represents a digital and pervasive ambient created by the convergence of the technologies of radio transmission and broadcasting (as an identification by radiofrequency (RFID), agents of software, sensor networks, processing of data by personal mobile devices, which provides, in cyberspace, the integration and the interaction of the devices named as «intelligent». This new reality, deeply enshrined in the very concept of «digital society», portrays an ambient (digital and intelligent) in which people are surrounded by intuitive interfaces embedded in every corner (even the most inhospitable ones) of a city (ranging from London to New York) or country, giving rise to the well-known «National surveillance state».

Make no mistake: Massive tons of our personal data are being captured, stored, processed and disclosed to unidentified third parties as we speak. The real problem lies in the ulterior usage of that vast array of personal data and, foremost, to what ends. Concretely, in cases of data breaches. This paper avowedly asserts that in such cases consumers (pursuant a data breach) have a natural right to seek redress and compensation from courts based on the damage of loss of chance of exclusive control of one´s personal data.

Keywords: Digital ambient; Digital society; National surveillance state; Big data; Data breach; Privacy; Loss of chance of exclusive control of one´s personal data; Natural right; Right to be left alone

Introduction

Privacy, a natural right

Not long ago, Professor Jack Balkin asserted that humankind had surpassed the threshold of the «Pretty Good Privacy» (PGP). In his insightful view, we (humankind) currently live in a so-called «National Surveillance State», in which the core of our natural rights (such as privacy [1], preservation of one´s self-image [2], and undeniable «right to be left alone [3]») are being progressively eroded. Privacy [4], «right to be left alone» [5] and «reasonable expectation of privacy» [6] are increasingly becoming a glimpse of the past, as the «analogic society» steadfastly faded away.

Swiftly heading towards an overarching «global-digital society», humankind faces candent challenges which rests upon the following conundrum: how to ascertain the boundaries of the murky circuit of Big data controlled by *surveillance intermediaries* (Facebook, Microsoft, Google, Ebay, Twitter, Yahoo!, We Chat, Apple)? In cases of data breaches, have citizens the right to seek redress from fiduciary data holders? If so, in what grounds? These questions are currently pressing in European Union, mainly from data protection [6] and cloud computing [7] standpoint.

This paper adamantly argues that data breaches should not prevent consumers (by definition, all of us) from seeking appropriate compensation from identified enterprises who were fiduciary holders of their personal data. The reason for this axiom rests upon a natural right [8] to not only gain access to fragments of their individuality, subjectivity and intimacy (in short, personal data), but uttermost the natural right to control [9] the universe of personhood [10] deeply ingrained in their personal data [11]. Consumers or citizens ought to be given the natural right to choose when, how, to whom, and to what purposes their personal data can be disclosed to third parties. Conversely, in the wake of data breaches, consumers ought to be given the right to seek compensation from fiduciary data holders. That is paramount as for constituting a stronghold that protects consumers from the lingering perils of the digital society we live in.

Privacy ought to be regarded as citizens´ natural right. This approach stretches far beyond the mere juxtaposition between privacy and fundamental rights [11]. Fundamental rights are mainly awarded within the scope of a Constitution [12]. Fundamental rights boundaries arise from a document endorsed by a given electoral majority in a given historical moment [13]. Fundamental rights are document-borne rights [14,15]. Antithetically, in our view, natural rights (for instance, privacy in the digital society in which we live in) are person-borne rights. Natural rights precede fundamental rights. As a result, natural rights are not a grotesque product of a capacious (or narrow) generosity of an array of lawmakers or legislators in a given historical time frame. Natural rights (such as privacy) do not depend on the circumstantial endorsement of lawmakers or legislators. Why? Natural rights are grains of personhood. Natural rights (such as privacy) erupt on digital society whenever a person born. Natural rights are particles of citizen's undeniable and unique subjectivity that Constitutions (let alone laws) ought to be unable to tear apart. Data breaches dissolves those seeds of citizen´s unique and unrepeatable personhood. Digital society brought along a multitude of benefits to humankind, but that wide range of social prosperity cannot tarnish or squander citizens´ unique personhood every time a data breaches surfaces. Conversely, citizen´s ought to be able to seek redress or compensation whenever a data breach occurs. The following remarks ought to provide apposite scientific grounds for that truism.

***Corresponding author:** Hugo Luz dos Santos, Magistrate Public Prosecutor (Portugal), International Legal Advisor, 聯邦大廈749號R/C, Macau, China, Tel: (+853) 655 27 671; E-mail: hugo.miguel.luz@gmail.com

Received May 09, 2018; **Accepted** May 15, 2018; **Published** May 18, 2018

Citation: dos Santos HL (2018) They See You and Yet You Don't See Them: Privacy in the Multilayered National Surveillance State Realm: A Dystopian Digital Society? J Comput Sci Syst Biol 11: 200-216. doi:10.4172/jcsb.1000273

Original public meaning of privacy in the digital society: also a human right and a fundamental right

As previously asserted, privacy in the scope of digital society is not only a natural right, but a human right [16], as embeds an undeniable intention of promoting it (privacy) to an uttermost level: the human rights level (Menschenrechte zu positivieren) [17]. Privacy is arguably wrapped under the cloak of a human right [18,19].

This approach begs the question: Being both a natural right and a human right [20], how can one ascertain [21] the original public meaning [22,23] of privacy on the brave new world of digital society?

Interpretation [24,25], as asserted by Jack Balkin, should begin with ascertaining the original public meaning [26,27] of privacy [23].

A thin theory of original public meaning [28,29] is not about how people at the time of adoption of U.S. Constitution [27,30] would have expected that the text would be applied to concrete situations [31], as in pre-internet era (analogic age) digital society was still crawling, rehearsing some «baby steps». Rather, it is about how people who lives in the digital society of 2018 would have expected that the text would be applied to concrete situations in which data breaches happens in a regular basis. This opens the door to the following axiom: pursuant to their quest to be kept alone and «unaccounted», citizens (now and then) expect that there is an unreachable core of privacy that is not to be violated by fiduciary data holders or, overarching, surveillance intermediaries, such as Facebook, Microsoft, Apple, Ebay, Google, Microsoft, Twitter, Yahoo, Instagram, Snapchat.

This account of original public meaning [32] is at all sensitive to the actual understandings of actual people living [23,33] at the time of United States, it will pick up these disagreements about meaning [34,35] (especially from those with different cultural backgrounds), and it will have to decide what to do with them [36,37]. One way we might deal with this problem is to pick a version of original public meaning [23] that is the least sensitive to these differences [38] in understanding [39], and that focuses as much as possible on areas of likely and overwhelming agreement [23] or overlapping consensus [40,41] being that the axiom which states that privacy is a human right, regardless of citizens´ cultural background, and no efforts should be spared to fulfill such an eminent right. That is why, for example, Balkin argues for a relatively "thin" theory of original public meaning-essentially confined to the original semantic meaning of the words [42], but taking into account any generally recognized terms of art, and *any background context* necessary to understand the text [43,44], such as the burgeoning development of digital and computerized technology brought along by digital society, which poses sizable challenges on privacy mainly from the its protection standpoint [44].

Although originally a natural and human right, privacy can also be seen through the lens of a fundamental right. However, at the time of the enactment of U.S. Constitution privacy had a glaringly different scope and range when compared to 2018, a vivid receptacle of digital society. Privacy harkens back pre-internet era, but arguably did not encompass a wide range of perils associated to the then inexistent digital and computerized society we live in.

Accordingly, what a thin theory excludes from original public meaning of privacy is the original expected application of the text-how people at the time of adoption of U.S. Constitution would have expected that the text (enshrining right of privacy) would be applied to concrete situations [45], as in the pre-internet era massive data breaches occurred on the realm of digital society were definitely not an issue (let alone a major one) back then. One can foresee that original public meaning of privacy does vary over time. This is paramount if one endeavors to ascertain the boundaries of privacy in the pre-internet era and of digital society we live in.

Original public meaning of privacy in the pre-internet era had a distinctively different scope if squarely compared to 2018. Protection of privacy in the pre-internet era had conspicuously dissimilar boundaries and a markedly narrower scope. Pre-internet era and analogic age have provided humankind the very last scent of nearly-unshakable privacy. Concerns about privacy (though existent) were not pressing. Concerns about privacy are much more pressing in 2018 (the perimeter of digital society) than ever before, as the boundaries between private sphere and public sphere are becoming increasingly evanescent. Judges´ and lawmaker's functional attention ought to be driven towards the protection citizens´ privacy on the confines of digital society. They are the very last bastion of defense in regard of the tutelage of citizens 'privacy on this frantically data-driven world we live in. One cannot stress this truism vigorously enough.

Protection of privacy in 2018 is a rather pressing issue amid intrusive government surveillance on the brave new world of digital society. Pervasive government surveillance seemingly has no bounds. Protection of privacy appears to be intertwined with an overlapping consensus [44,46,47] that enshrouds the axiom that an unassailable right to be left alone in the digital society is not a moral conception [48-51], but a conception of justice [52,53].

A conception of justice (for privacy) is currently more pressing than ever before, especially in light of atrocious events (9/11), which have pushed the core of our natural, human and fundamental right of privacy to nearly-hollow standards, giving rise to the so-called «National Surveillance State». «National Surveillance State» is the original public meaning of privacy in 2018.

Multilayered National surveillance state on the brave new world of digital society: perils to the natural right of privacy

«National Surveillance State» [54] is an expression coined by renowned doctrine a decade ago. This expression stems from a rather polymath approach: world we live in has changed dramatically since 9/11 events.

Prior to the unfortunate events that have taken place in 9/11, liberty and privacy (though subject to restrictions) were seemingly bullet-proof rights. Closely regarded as airtight rights. 9/11 brought along an atmosphere of unbearable suspicion, which has given rise to a widespread suppression of liberties and rights. Being discernably close to a far-reaching paranoia arisen from those hapless events, privacy has been caught on the middle of a callous and often ferocious battle between safeguarding security and harboring some civil rights.

In the aftermath of 9/11 events, balancing or squarely aligning those conflicting rights is a rather herculean task. No surprise stems from the fact that overall governments have chosen to confer priority to security, often wrapped under the seeming (yet real?) cloak of «public common good». As a result, privacy´s core has been severely weakened to historical minimum standards.

This abhorrent trend has been shrewdly portrayed by acclaimed doctrine [55]. Ranging from intercepting phone calls in real time to capturing footage amid a rather oppressive surveillance [56], governments have conspicuously interfered on the core of citizen´s liberties and rights worldwide.

The «brave new world» of digital society, constituted by a remarkable electronic and technologic apparatus, has somehow heightened the degree of intrusion on citizen´s private sphere.

Unsurprisingly, «we hear them in the media, which is buzzing with stories about government information gathering, such as the Total Information Awareness program, the airline passenger screening program, and the surveillance of people's phone calls conducted by the secretive National Security Agency. We hear them made by politicians and security officials. And we hear them made by judges deciding how to balance security measures with people's constitutional rights.

These arguments are part of the debate between privacy and security. The consequences of the debate are enormous, for both privacy and security are essential interests, and the balance we strike between them affects the very foundations of our freedom and democracy. In contemporary times especially after the terrorist attacks on September 11, 2001-the balance has shifted toward the security side of the scale»[56].

When it comes to pursuing the so-called «national security», or in a more polished manner «greater good», governments seem to have no restrictions whatsoever in order to accomplish the goal of security, as citizen´s personal data is being captured, stored, and processed (sometimes for abstruse and spurious ends) at an alarming rate with little regard for surveillance transparency [57]. Digital society is seemingly governments' «tip of the spear» when it comes to «getting things done» swiftly and in a purely veiled manner: they see you and yet you don't see them.

In the same vein, «the government has been gathering more information about people and engaging in more surveillance. Technology is giving the government unprecedented tools for watching people and amassing information about them—video surveillance, location tracking, data mining, wiretapping, bugging, thermal sensors, spy satellites, X-ray devices, and more. It's nearly impossible to live today without generating thousands of records about what we watch, read, buy, and do—and the government has easy access to them» [58].

But of course there are consequences associated to this data-driven «surveillance streak» [59], as «the privacy-security debate profoundly influences how these government activities are regulated. But there's a major problem with the debate: Privacy often loses out to security when it shouldn't. Security interests are readily understood, for life and limb are at stake, while privacy rights remain more abstract and vague. Many people believe they must trade privacy in order to be more secure. And those on the security side of the debate are making powerful arguments to encourage people to accept this tradeoff» [58].

Digital society coupled with local crisis with global impact have profoundly impacted the way governments perceived the inner and outer limits of natural right of privacy. Local crisis with global impact (such as 9/11 events) have created perfect opportunities to maximize security concerns and minimize privacy concerns. 9/11 was the «perfect storm» that enabled the former and thwarted the latter to very minimum standards. Not just that though. Being reduced to historical minimum standards, privacy becomes a «diffident right», as it would be always subjected to technocratic rationalizations, sudden (yet functionalist) shortages, and uncountable reductions from governments worldwide aimed at attaining an ultimate purpose: impenetrable security. On this dystopian view, privacy´s realm is inversely proportional to security´s: the broader are the horizons of the latter, the narrower are the boundaries of the former. Governments have seized local crisis-borne opportunities with overwhelming prowess. Digital society is the perfect tool to pursuing this quest for a permanent and totalitarian security on the realm of a (still imperceptible) digital-totalitarian state. No wonder renowned doctrine has baptized this obnoxious trend as «National Surveillance State».

The aforementioned assortment of remarks begs the question: how did we get here?: As argued by renowned doctrine «late in 2005, the New York Times reported that the Bush administration had ordered the National Security Agency (NSA) to eavesdrop on telephone conversations by persons in the United States in order to obtain information that might help combat terrorist attacks. The secret NSA program operated outside of the restrictions on government surveillance imposed by the 1978 Foreign Intelligence Surveillance Act (FISA) and is thought to be only one of several such programs. In 2007, Congress temporarily amended FISA to increase the President's power to listen in on conversations where at least one party is reasonably believed to be outside the United States. In June 2008, Congress passed a new set of amendments to FISA, which allow the President to engage in a broad range of electronic surveillance without seeking warrants against particular individual targets of surveillance. At the same time, Congress effectively immunized telecommunications companies that had participated in the secret NSA program» [60].

In order to capture the kernel of this surveillance streak, one ought to summon the luggage of memory: History and war on terror. 9/11 events have provided a germane opportunity to the rising of an irrevocable outbreak of government´s pervasive surveillance. As a result, this tandem gave rise to national surveillance state, a murky way of governing.

One should put forward the first level of national surveillance state´s main features which, as previously asserted, date back 9/11 events: «The secret NSA program and New York's Lower Manhattan Security Initiative reflect a larger trend in how governments do their jobs that predates the September 11, 2001 attacks and the Bush administration's declaration of a "war on terror." During the last part of the twentieth century, the United States began developing a new form of governance that features the collection, collation, and analysis of information about populations both in the United States and around the world. This new form of governance is the National Surveillance State. In the National Surveillance State, the government uses surveillance, data collection, collation, and analysis to identify problems, to head off potential threats, to govern populations, and to deliver valuable social services. The National Surveillance State is a special case of the Information State-a state that tries to identify and solve problems of governance through the collection, collation, analysis, and production of information» [58].

War on terror and National Surveillance State might just be a beloved and caring couple. National Surveillance State spans far beyond the mere emergence of a seasonal (thus revocable) war on terror though. National Surveillance State takes appropriate advantage from the perks of digital society we live in. National Surveillance State is actually wagering on the fringe benefits of digital society and its accompanying cutting-edge technology. National Surveillance State is a permanent (though imperceptible) condition and is not going anywhere. Like previously pointed out, is an inauspicious way of governing. Get used to the «new normal».

As asserted by Prof. Jack Balkin «the war on terror may be the most familiar justification for the rise of the National Surveillance State, but it is hardly the sole or even the most important cause. Government's increasing use of surveillance and data mining is a predictable result of

accelerating developments in information technology. As technologies that let us discover and analyze what is happening in the world become ever more powerful, both governments and private parties will seek to use them» [61].

Additionally, «the question is not whether we will have a surveillance state in the years to come, but what sort of surveillance state we will have. Will we have a government without sufficient controls over public and private surveillance, or will we have a government that protects individual dignity and conforms both public and private surveillance to the rule of law? The National Surveillance State is a way of governing. It is neither the product of emergency nor the product of war. War and emergency are temporary conditions. The National Surveillance State is a permanent feature of governance, and will become as ubiquitous in time as the familiar devices of the regulatory and welfare states. Governments will use surveillance, data collection, and data mining technologies not only to keep Americans safe from terrorist attacks but also to prevent ordinary crime and deliver social services.' In fact, even today, providing basic social services-like welfare benefits-and protecting key rights-like rights against employment discrimination- are difficult, if not impossible, without extensive data collection and analysis. Moreover, much of the surveillance in the National Surveillance State will be conducted and analyzed by private parties» [62].

Given this heinous trend, doctrine is championing for a sort-of democracy-sedition stating «the most obvious way that citizens of a democracy could influence surveillance policy would be to elect reform-minded leaders» [62].

This doctrine is advocating for government surveillance resistance which ought to uphold privacy instead of security stating «the ability of everyday Americans to resist and alter the conditions of government surveillance. Americans appear to have several avenues of resistance or reform. We can vote for privacy-friendly politicians, challenge surveillance in court, adopt encryption or other technologies, and put market pressure on companies not to cooperate with law enforcement» [62].

Nevertheless, the real problem lies elsewhere: citizen´s personal data gathered through veiled but prolonged surveillance, which is enabled by a meddling and immeasurable National Surveillance State, is nowadays carried out by private parties [63] with limited or inexistent regulatory oversight [63]. This is the second level of National Surveillance State. On the third level of National Surveillance State, Surveillance intermediaries' activities like Facebook, Ebay, Google, Wikipedia, Twitter, Apple, Snapchat, Yahoo, constitute a striking example of much-needed «legislative measures taken against online intermediaries»[63-65], as their functional activities (when it comes to «corporate surveillance») is conveniently wrapped in opaqueness. Secondary use of big data [66] carried out by surveillance intermediaries constitutes a conspicuous (yet unsurprising) example of that.

In the meantime, one should emphasize that the degree of pervasiveness augments every time governments add identified players (yet suffused with unidentified and hazy purposes) [67,68] on the breadth of National Surveillance State [64]. One should deem this as a multilayered National Surveillance State. This novel Leviathan [69] can be straightforwardly depicted by the following manner: on the very first layer of National Surveillance State, governments perform steady and irrevocable surveillance on their citizens (placidly collecting the perks of digital society and from its inseparable counterpart, cutting-edge technology) aimed at gathering information (personal data) which ought to prevent future events (such as terrorist attacks and similar nefarious endeavors).

The government targets persons under section 702 of the Foreign Intelligence Surveillance Act [70] (FISA), conceivably the most relevant statutory authorization for government surveillance present-day, by «tasking,» or targeting for collection, a «selector,» or a specific phone number, email address, or other communications facility [71,72]. This allows the government to intercept all communications «to» or «from» a selector [73] and, to some extent, perform cross-border data access [74] or even off-shore data storage [74].

In so doing, the frontiers of the known (the collection, storage of citizen´s personal data to accomplish an allowable goal, national security or, more diffusely, «greater good») and frontiers of the unknown (processing, disclosing and ulterior dissemination of personal data to unidentified third parties for shady ends) become increasingly blurred: being professedly captured and collected for condonable ends (raising security levels in order to quash imminent threats to national security), are we really sure that bunch of information is being processed and disseminated to solely attain those purposes? [75].

Or, quite the opposite, that vast miscellany of information (a true medley of private and public information) [76] is being also conveyed to accomplish other spurious ends, such as ascertaining our life-style, habits, inner attitudes, or, at a terrifying level, political or sexual preferences? Does that means private information captured on a public environment is to be subtracted from citizen´s control for good? [77].

As outlined above, further to the emergence of National Surveillance State, the lines between public sphere, intimate sphere, and private sphere [78] became increasingly dimmed [79], as knowing the exact boundaries of each one of those spheres constitutes the riddle of twenty-first century.

In the process, principle of human dignity, a quintessential feature of United States of America Rule of Law, and which ought not to be impaired by a technocratic and heartless cost-benefit analysis [80-90], is steadily fading away [91].

Multilayered National surveillance state on the Realm of Digital Society: The Burgeoning Preponderance of Surveillance Intermediaries: Quasi-Governmental Actors?

To the extent governments perform invasive surveillance programs that corrodes citizen´s privacy [92], the degree of ubiquity of these technology-enabled surveillance tools heightens [93] at the very same pace that governments bestows a duty of collection, storage, processing and dissemination of information (that is to say citizen´s personal data) to private parties placed on the second level of National Surveillance State. Governments expect full and unrestricted cooperation from selected private parties [94], in regard of capturing and disclosing citizens´ pertinent personal data [95]. Most of the times (if not always) [96] governments do get that fully expected cooperation [97].

However, an hazard looms

Abnormal partnerships between governments and private parties aimed at collecting, storing and processing citizens 'personal data can provoke damage to the unreachable core of citizens 'privacy [98]. Yet a concrete danger surfaces on the third level of National Surveillance State when a strategic misalignment [99] between Surveillance intermediaries or online intermediaries («quasi-governmental actors»

[64] or, to some extent, «corporate avatars») [74] and governments occurs though [100,101]. Worse yet, when online intermediaries adopt a belligerent and rather contentious vein against governments in the era of Internet of Things [102].

This brings us to the third layer of National Surveillance State: Unlike the second level of National Surveillance State in which private parties aid governments to pursuing condoned ends of collecting information to prevent terrorist attacks, surveillance intermediaries or online intermediaries somehow constrain the accomplishment of those ends by concealing crucial information from governments [103].

On the third layer of National Surveillance State, the erosion of privacy boundaries is far more damaging to citizen´s right of informational self-determination [104], as the unavailability to gain access to the batch of information withheld by surveillance intermediaries will only give rise to more government surveillance, thus corroding even further citizens 'privacy and opening a «new age of threats» [105]. Simply do the math: more surveillance corresponds symmetrically to less privacy. In the process, so much for the tradeoff security-privacy [106], as (even) more government surveillance ought to override privacy´s minimum standards in the long-term.

This stems from the axiom that not only Surveillance intermediaries activities' lack regulatory oversight, but mainly due to the fact that governments are clueless about the extension of surveillance undertaken by online intermediaries. In short, this three-folded or multilayered National Surveillance State is potentially disruptive for citizens 'privacy as both governments and citizens are unaware of the depth and range of surveillance programs performed by online intermediaries. Currently, this murkiness has given rise to a declared battle between governments and surveillance intermediaries over the control of personal data collected in electronic portable devices [107], such as IPhones: Apple´s high profile 2016 legal battle in which the company frantically challenged a court order «commanding it to help unlock the iPhone of one of the San Bernardino terrorists» [108], portrays how central the question of regulating government surveillance [109] has become in United States of America´s politics and law [110].

Does really such thing (surveillance intermediaries) exists? If so, what really are Surveillance intermediaries or online intermediaries?

As so well asserted by reputable doctrine «although the digital age has broadened the horizons of government surveillance, it has also imposed constraints on account of its political economy: the technological, commercial, political, and cultural arrangement of our digital infrastructure. By entrusting our data processing and communications to a handful of giant technology companies, we've created a new generation of surveillance intermediaries: large, powerful companies that stand between the government and our data and, in the process, help constrain government surveillance. Far from an anomaly, the fight over the San Bernardino iPhone previews the likely new normal: a contentious relationship between the companies that manage our digital bodies and the government that protects our physical ones. Surveillance intermediaries like Apple (and Google and Facebook and Microsoft) have the incentives and means to meaningfully constrain government surveillance. They do so both by their own lights and by subjecting government surveillance to greater checks from within the government itself» [111].

Make no mistake: when it comes to capturing, storing, withholding and mostly controlling citizens 'personal data, Surveillance intermediaries (who carries out proper «corporate surveillance») [110] hold a sizable power. That power is not restricted to that though. Championing for civil rights (such as privacy) is becoming increasingly trendy amongst surveillance intermediaries, «as Verizon, which owns Yahoo, signed on to an amicus brief on behalf of leading tech companies in the pending Supreme Court case Carpenter v. United States, arguing that the Court should extend Fourth Amendment protections to geolocation data» [110,112].

Surveillance intermediaries´ substantial power brings along an immediate danger: the interplay between «government surveillance» and «corporate surveillance» can be often counterproductive and even more damaging to citizens privacy: «at the first stage, surveillance intermediaries can help society better construct surveillance frontiers-menus of surveillance policy options-by adding more information and more diverse perspectives, as well as by minimizing inefficient alternatives. But they can also create negative second order effects by forcing the government to engage in more intrusive surveillance and by making it easier for the surveillance intermediaries themselves to collect more data on their users» [113].

Being an axiom that Surveillance intermediaries hold a rather robust power, which enables them to constrain government´s surveillance agenda, question is to fathom its real depth and extent or, more prosaically, «how» and «when» they exercise this power.

A surveillance intermediary is typically a party that collects massive tons of sensitive information, customarily for its own business purposes, that the government wants for example, phone company billing records that contain a cellphone subscriber's call history background. Instead of delving information from the target directly (specified agglomeration of citizens or persons of interest in a given criminal investigation), the government seeks it from the third party, either because it's far easier to get the information that way or because only the third party has the information [114]. The third party becomes a surveillance intermediary: it stands squarely between the government and the target of the surveillance [115]. As a result, government surveillance and corporate surveillance (truly middlemen or gatekeepers) creates multiple layers of surveillance in which every side conceal information from each other and, worse, with limited or inexistent regulatory oversight.

This approach begs the question: How on earth this mighty power (held by surveillance intermediaries on the third level of National Surveillance State) surfaced on digital society perimeter in the first place? A logical cause stems from enhanced network effects. Because of enhanced network effects (digital platforms become increasingly valuable as more and more people use them for lengthy periods of time) and economies of scale, an exiguous number of industry giants dominate among these middlemen and gatekeepers. Just three companies-Google, Microsoft, and Yahoo-dominate 98% of the U.S. search engine market [115]. A couple of video streaming services, such as Netflix and YouTube, consume over half of the downstream fixed access bandwidth during pinnacle periods in North America [116]. That generates an indomitable sway on the digital society we currently live in. Prosaically, creates real (yet boundless) power.

Moreover, «the average Facebook user spends close to an hour every day using Facebook services-and that's before you include Facebook-owned WhatsApp. What's true of platforms applies to devices: 97% of U.S. smartphones run either Google's Android or Apple's iOS. Ultimately, the biggest surveillance intermediaries dominate not just the internet but also the global economy. Five U.S. technology companies-Apple, Alphabet (Google's parent company),

Microsoft, Amazon, and Facebook-routinely have the biggest market capitalizations in the world» [117].

This creates an immense stronghold of information akin to a quasi-governmental power for surveillance purposes. One can deem this as a corporate digital-borne power, a dystopian ramification of the digital society we live in. They are not going anywhere too. If anything, corporate digital-borne power will likely continue to grow.

This boundless «corporate digital-borne power» would do very little to curtail government surveillance if surveillance intermediaries saw their interests as aligned with those of government spies and investigators [117]. But that is quite often not the case. Today's surveillance intermediaries have powerful incentives or enticements to resist government surveillance [117]. In this regard the 2013 Snowden disclosures were a sizable turning point. The gigantic leaks of classified information imparted a boundless surveillance system-and, worse, implicated (on the second level of National Surveillance State) major Silicon Valley companies as collaborators, «causing blowback from domestic civil liberties groups and overseas customers» [117]. Although the disclosures paved the way to some legislative and policy changes, they didn't alter or revamp the gist of United States surveillance [117]. They did, however, as Julian Sanchez emphasizes, «transform the incentives of the technology companies that maintain [the] architectures that permit surveillance» [117]. This is arguably Edward Snowden's cardinal victory to augment the inducements for surveillance intermediaries to antagonize the government [117].

What sort of incentives (if any) do surveillance intermediaries have to resist government surveillance? These incentives fall into two sort of categories. The first is markedly financial. Companies have always had the incentive to lower compliance costs by resisting government surveillance (as long as the costs of such resistance were themselves not too great) [118]. «But the Snowden disclosures have turned such resistance into an opportunity for product differentiation. For example, when Apple publicly touts how its business model doesn't need to access user data, part of what it's doing is jabbing at companies like Google and Facebook, which rely on scanning user data to sell advertisements» [119].

Besides, resisting U.S. government surveillance can also ameliorate a company's overall competitiveness—sharply, its ability to sell its products and services elsewhere, including abroad [119]. This is overridingly important «because the international market provides the bulk of sales for modern technology companies (unlike for the phone companies and retail banks that made up the earlier generation of surveillance intermediaries)» [120]. For instance, Almighty Facebook has over two billion active monthly users, of which the overwhelming majority are located outside the United States of America; likewise, «over half of the company's ad revenues come from abroad» [119]. «Given such globally distributed revenue streams, along with the ability to move their key asset data instantaneously around the world» [121], today's surveillance intermediaries are akin to a Platonic ideal of a multinational corporation [121].

This scenario depicts surveillance intermediaries (on the third level of National Surveillance State) as quasi-governmental actors by implementing self-governance systems and rules to unilaterally regulate the conduct of their users (consumers, by definition us all) and governments, again, with limited or inexistent regulatory oversight. Yet, unlike the government surveillance, they are not subject to any constitutional limitations or democratic controls whatsoever [121]. The information that surveillance intermediaries glean can be used to «generate a fastidious record» of consumer transactions and «personalize every aspect of the interaction» with the marketplace [121], thus eroding our beloved and sacred privacy every step of the way.

Multilayered National Surveillance State and the Balance of Power between Law Enforcement Government Agencies and Surveillance Intermediaries: The Importance of the Principle of Proportionality and of the Principle of Human Dignity on the Tradeoff Security-Privacy

Digital society and Multilayered National Surveillance State, especially at the third level, stands at crossroads: should societal interest in granting national security through security surveillance supersede protection of privacy by enabling governments to gaining access to encrypted systems? [100] Antithetically, should surveillance intermediaries continue to opposing certain forms of government surveillance [122] «employing default encryption technologies [123] on mobile devices and explicitly marketing them as being impervious to government snooping»? [124].

Concretely, how can one manage to strike a balance between societal interests in chasing «bad guys», pursued by government's law enforcement agencies, with the egoistical interests pursed by mighty corporations or surveillance intermediaries? [125] On the previously asserted cases of strategical misalignment between law enforcement government agencies and multinational corporations (just like the one occurred in San Bernardino terrorist attacks), one should refer to the prototypal principles of proportionality and human dignity.

Throughout this manuscript I have been championing for protection of citizens´ privacy from governments´ prying eyes. A vigorous defense for security concerns is seemingly contradictory at that glance. A cautious note comes in handy: one should not forsake that privacy cannot always prevail over security at any cost [126,127]. One should bear in mind that sometimes too much privacy can be as equivalent as opening the Pandora box of perennial insecurity with deleterious effects on the long-term common good – bullet-proof privacy can pave the way to even more vicious terrorist attacks which will give rise to an ever-present security, thus pushing privacy to a tokenistic value or inexistent one at all. Striking a delicate balance between principle of security and principles of proportionality and his «companion route» principle of human dignity is definitely a challenge that one should embrace. How can one accomplish such an arduous task? Displaying the pivotal value of principle of proportionality [128] coupled with the seminal principle of human dignity.

Principle of proportionality [129], which in recent decades achieved remarkable recognition in theory and practice of the control of constitutionality [130] consists of three subprinciples: adequacy, necessity and the proportionality in a strict sense [131]. These three lines express the idea of optimization [132,133], a precious asset when it comes to balancing seemingly conflicting principles [134] or, in a broader sense, opposing interests [135], such as the ones pursued by law enforcement government agencies and surveillance intermediaries.

Conflicting principles (impervious security and privacy, inextricably linked with the principle of human dignity), require a constant optimization in relation to what is factual e legally possible [136]. Sub principles of adequacy and of necessity refer to the optimization concerning the existent factual possibilities (gathering

information from surveillance intermediaries pertaining to a criminal event)–on our lens, it suits perfectly in the sphere of surveillance intermediaries the share of information with government agencies of law enforcement, for purposes of prevention and repression of terrorist attacks provided that the sharing of that information is restricted to personal data solely related with criminal events. From that point onward, principle of security ought to submerge and the principle of human dignity (which wraps the inner and outer limits of privacy) ought to emerge at his maximum height.

Sub principle of proportionality in a strict sense refers to the optimization concerning the legal existent possibilities in U.S. legal landscape - meaning, legal compromises between radically opposing principles which are sufficiently ingrained in the legal system of the United States of America [137-139].

In this light, the share of information for purposes of prevention and repression of terrorist attacks, passes the test of proportionality (*Verhaltnismaβigkeitsgrundsatz*) [140] whenever information gathered from electronic devices has conspicuously clear criminal relevance in regard of prevention or repression of terrorist attacks. On this point (and on this point only) principle of security surpasses the principle of human dignity [141], which is the dogmatic mantle of privacy [142].

In this regard, one ought to summon the third subprinciple of proportionality, which is of the proportionality in the strict sense. This subprinciple expresses the weighing [143] about the existent legal possibilities [144,145]. It corresponds to a line that can be named as «Law of Weighing» [146]. This line says: «The higher the degree of non-fulfillment or allocation of a principle, the greater must be the importance of completing the colliding principle» and under that (the Law of Weighing) a «Weight Formula» [147] defines the specific weight of all colliding principles» [148].

In this case the «Law of Weighing» [148] and of the «Weight Formula» [149], both determine that the prevailing principle (principle of security and societal common good, which enables law enforcement agencies to gather information from surveillance intermediaries aimed at the prevention and repression of terrorist attacks) preserves the non-prevailing principle of human dignity [150] (which encompasses the right of privacy, which has no absolute nature) [151] to fairly acceptable standards [152].

At this glance, a balanced portray of the paramount importance of principle of proportionality [153-155] («minimal impairment test of the protected rights» of citizens 'privacy) [156] and «the least restrictive alternative» [157] have been depicted, and, in the process, privacy´s acceptable standards have been safeguarded.

Multilayered National Surveillance State and Standing on Surveillance Cases and of Data Breach Cases: State of Art in United States of America

Data breaches of citizen´s personal data is one of the most pressing issues arisen on the breadth of digital society. Aimed at corroborating that one ought to put his eyes at «Cambridge Analytica case», in which data breaches were allegedly enabled by Facebook´s lack of due diligence: «Facebook is facing international investigations into the illicit harvesting of users' personal data. The information was collected by Cambridge Analytica, a political consulting firm that backed President Trump's 2016 election campaign. According to a whistleblower, Cambridge Analytica gathered data from 50 million users (a figure that Facebook has now admitted could be as high as 87 million), then developed a software program that profiled these citizens to predict voting patterns – and, through micro-targeted ads, influence US citizens' voting decisions» [158].

«Cambridge Analytica case» is a striking example of citizens´ secondary use of personal data. Typically, information circuit rests upon the following scheme: i) invasions (intrusion; decisional interference); ii) data subject; iii) information collection (surveillance; data mining [159-162]; interrogation); iv) information processing (aggregation; identification, insecurity; secondary use, exclusion); v) information dissemination (breach of confidentiality; disclosure; exposure; increased accessibility; blackmail; appropriation, distortion) [163]. Ascertaining accurately each one of these outlined doctrinal category goes far beyond the scope of this manuscript.

What is secondary use of data? Secondary use of data [164] «is the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent (.....) Secondary use can cause problems. It creates a dignitary harm, as it envolves using information in ways to which a person does not consent and might not find desirable. Secondary uses thwart people's expectations about how the data they give out will be used. People might not give out data if they know about a potential secondary use (.....). The potential for secondary use generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability. In this respect, secondary use resembles the harm created by insecurity. The harm is a dignitary one, emerging from denying people control over the future use of their data, which can be used in ways that have significant effects in their lives» [165].

Secondary use of data is deeply intertwined with Article´s III [166] Standing on data breach cases, as just like it happened in Cambridge Analytica case, there has been a vast array of Facebook´s user's personal data that was unduly conveyed for a purpose (a markedly electoral one) completely unrelated with the primitive purpose of collection of data.

On another angle, United States Supreme Court´s decisions, unlike European Court of Human Rights [167] (ECHR) [168,169] and Court of European Union (CEU) [74,170], have been putting forth insurmountable high standards in regard of Article III Standing in Surveillance cases [171].

U.S. Supreme Court upholds the Standing Test [172]. Accordingly, U.S.C. burdens a plaintiff with proving (beyond reasonable doubt?), at the very least [173], that she has «(1) suffered an injury in fact», (2) «that is fairly traceable to the challenged conduct of the defendant» [174], and (3) «that is likely to be redressed by a favorable judicial decision» [175].

These requirements oftentimes set an unconquerable high bar [174] for putative Surveillance plaintiffs, who endeavor to prove that they have indeed suffered a deemed «injury in fact» [176] that is «certainly impending» when most of the evidence that would tend to prove that fact is classified» [177].

United States Supreme Court´s stance on Article III [74,178] Standing in Surveillance cases may have recognized the threat of a systematized governmental surveillance that can impose on a citizenry [74], but have failed bluntly as to deliver the duly needed protection to citizens that have been subjected to a long-term and pervasive surveillance: «The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power» [179].

U.S. Supreme Court and Federal Courts stance on Surveillance cases constitutes a fine example of this jurisprudential trend. In Laird

v. Tatum [180] «found insufficient evidence of harm to support the plaintiffs' claim of excessive (and permanent) [181] government surveillance, it also noted its recognition of «constitutional violations» arising from the «deterrent or «chilling» effect of governmental regulations that fall short of a direct prohibition against the exercise of First Amendment rights» [182]

As outline above, this stems from the fact that United States Supreme Court and Federal Courts set out insurmountable high standards in regard of Article III Standing in Surveillance cases, thus hindering the success rate of claims in which plaintiffs (citizens/consumers) sought appropriate redress from the government.

The very same insurmountable high standards in regard of Article III Standing have been transferred to data breaches cases. Just take a look of what is happening on the scope of federal class actions. This issue is not a small one. The burgeoning digitalization of our personal data has created corresponding increase in the bulk of electronically stored private information in the domain of third parties [183]. That private information is at risk of theft, loss, or manipulation by unidentified third parties, generally hackers, whose intentions are far from being merely angelical. When hackers attack and subtract citizen's personal data, «victims often band together in federal class actions, naming the custodians of their private data as defendants» [184]. However, «district courts are dismissing these class action claims at the doorstep for lack of Article III standing. The corporate defendants argue, and many courts agree, that a plaintiff's alleged increased risk of future data misappropriation is insufficient to satisfy the U.S. Supreme Court's test for an "injury in fact," a critical component of the traditional standing analysis» [185].

Asymmetrically, eulogized scholars argued that plenty of consumer´s data breach class actions indeed satisfy the Supreme Court's standing requirements, as outlined in the Court's 2013 decision in Clapper v. Amnesty International USA [186] and its 2016 decision in Spokeo, Inc. v. Robins [186]. More on this later.

As argued by Professor Nicholas Green, with a colossal amount of data storage comes increased risk «that thieves and rouges, from both inside and outside a custodian entity» [186], will breach the security protecting individual personal information. [187] «Because the federal Class Action Fairness Act ("CAFA") provides a lower threshold for Article III diversity jurisdiction in multistate class actions than in traditional diversity suits, many data breach cases are brought in federal district courts» [188]. As courts of limited jurisdiction [189], the district courts are required to make sure cases are properly before them as a threshold matter [189,190]. Among other required components of proper jurisdiction, plaintiffs ought to have standing to sue [191,192]. «Plaintiffs bear the burden of showing standing at every stage of litigation, and must allege sufficient facts to support their right to sue at the pleading stage or risk dismissal under Federal Rule of Civil Procedure 12(b)(1)» [193,194].

In data breach class actions, often the hardest aspect of standing for plaintiffs to adequately allege is that they have indeed suffered an «injury in fact». [193] In crux, plaintiffs must show that they themselves have suffered the violation of a legally protected right of privacy (personal data stolen or unduly subtracted from hackers), and that their harm (or, more commonly, injury) [193,195] «is neither hypothetical nor conjectural» [196].

In innumerable cases, data breach plaintiffs have not suffered actual desecration of their personal data, but are at major risk for future data malapropism [193]. «The federal circuits have split on the adequacy of a future misappropriation theory of injury in fact, with some finding standing and others dismissing suits for want of it» [197]. Plenty of district courts appraises the «future misappropriation theory in light of the 2013 U.S. Supreme Court decision in Clapper v. Amnesty International USA, which was decided in the context of a challenge to the Foreign Intelligence Surveillance Act ("FISA")» [193].

Overall, U.S. Courts have been rather dismissive in regard of data breach cases. This jurisprudential trend has been harshly criticized by renowned doctrine. Quite recently, Professor Daniel Solove and Professor Danielle Keats Citron have displayed their academic concerns in regard of this pressing matter [193]. Their joint research stated that «in lawsuits about data breaches, the issue of harm has confounded courts. Harm is central to whether plaintiffs have standing to sue in federal court and whether their legal claims are viable. Plaintiffs have argued that data breaches create a risk of future injury, such as identity theft, fraud, or damaged reputations, and that breaches cause them to experience anxiety about this risk. Courts have been reaching wildly inconsistent conclusions on the issue of harm, with most courts dismissing data-breach lawsuits for failure to allege harm. A sound and principled approach to harm has yet to emerge. In the past five years, the U.S. Supreme Court has contributed to the confusion. In 2013, the Court, in Clapper v. Amnesty International, concluded that fear and anxiety about surveillance-and the cost of taking measures to protect against it-were too speculative to satisfy the "injury in fact" requirement to warrant standing. This past term, the U.S. Supreme Court stated in Spokeo v. Robins that "intangible" injury, including the "risk" of injury, could be sufficient to establish harm. When does an increased risk of future injury and anxiety constitute harm? The answer remains unclear. Little progress has been made to harmonize this troubled body of law, and there is no coherent theory or approach» [193].

This doctrine have managed to pinpoint the crux of U.S. Court´s lack of consistency in regard of standing in data breach cases. They argue that «the difficulty largely stems from the fact that data-breach harms are intangible, risk-oriented, and diffuse. Harms with these characteristics need not confound courts; the judicial system has been recognizing intangible, risk-oriented, and diffuse injuries in other areas of law. We argue that courts are far too dismissive of certain forms of data-breach harm and can and should find cognizable harms» [198].

Criticizing recent U.S. Supreme Court´s decisions, Prof. Ryan Calo argued that «the vast majority of privacy harms fall into just two categories—one subjective, the other objective. The subjective category of privacy harm is the perception of unwanted observation. This category describes unwelcome mental states-anxiety, for instance, or embarrassment—that accompany the belief that one is or will be watched or monitored. Examples include the harm experienced by the tenants in Hamberger v. Eastman, the unease caused by a massive data breach, and the concern over generalized surveillance at issue in the Keith case and Laird v. Tatum» [198].

Splitting the two categories of privacy harms, Prof. Ryan Calo further asserts that «the objective category of privacy harm is the unanticipated or coerced use of information concerning a person against that person. These are negative, external actions justified by reference to personal information. Examples include the unanticipated sale of a user's contact information that results in spam and the leaking of classified information that exposes an undercover intelligence agent» [198].

In Prof. Ryan Calo´s approach, subjective and objective categories of privacy harm are «brothers in arms», but conserve its pristine

nature. The subjective and objective categories of privacy harm are different but related. Just as assault is the anticipation of battery, so is the perception of unwanted observation largely an apprehension of information ill-treatment. «The subjective and objective components of privacy harm are two sides of a well-worn coin: the loss of control over information about oneself or one's attributes» [199].

Although a risk of future harm was arguably anticipated by Courts in Robins v. Spokeo [199] when the Court noted that «intangible informational injuries, recognized at common law, can provide the basis for harm sufficient to support standing» [199], there is no guarantee that in the forthcoming future U.S. Courts will consider data breach cases worthy of redress. A new approach is duly needed in this domain.

Privacy Harm in Data Breach Cases (Identity Theft): Loss of Chance of Exclusive of Control of One´S Fragments of Personality as an objective, Absolute and Multiplied Privacy Harm

As previously pointed out, discussions have been put forth as to whether privacy harm is worthy of compensation or not. U. S. Courts have been rather dismissive of certain forms of data-breach harm. Cognizable harms have been rebuffed too.

From our point of view, privacy harm is an objective one. Privacy harm is not an intangible and far-fetched injury. Anxiety and unsureness as to whether personal data is going to be used in the future to the practice of misdeeds are an ulterior consequence of a data breach. Anxiety and unsureness are a subjective backlash of a data breach. They are not the privacy harm itself.

Anxiety and unsureness being an inward state are hardly the harm itself. Anxiety and unsureness are not palpable and cognizable at a judge´s lens. Quite the opposite, privacy harm is related with the free development of one´s personality in an objective sense. Every time a data breach occurs a fragment of one´s eminent and unique personhood is besmeared. Privacy harm consists of that subtraction of one´s unique and unrepeatable personhood. That unrepeatable personhood deeply ingrained in citizens´ personal data is objective and absolute. There is no such thing as repeated personalities or repeated personhoods. Privacy harm is objective because it is centered on the unique and absolute nature of one´s eminent personhood. Privacy harm is absolute because the personal data subtracted further a data breach belongs to a zone of exclusivity that no one should be allowed to interfere but the aggrieved citizen. The aggrieved citizen has the exclusive control of fragments of his undeniable, unique and absolute personhood.

This approach is squarely aligned with our starting point: privacy is a natural right. Privacy is a human right. Privacy is not (just) a fundamental right, always dependent on occasional or seasonal lawmakers 'good mood.

Being a natural right, privacy is inextricably linked with the objective and absolute value of human being. Personal data (thus privacy) are fragments of a one-of-a-kind human being that is not to be smeared, let alone in an unauthorized manner.

Identity theft constitutes a striking example of how an identity thief can begrime one´s unique and absolute personhood.

Identity theft cases are the hallmark of personality debasement. Every identity theft case has a stereotyped feature: identity thieves endeavor to erase a unique personality from digital society with multiple shots. Make no mistake: identity theft cases can produce a staggering amount of damage on the free development of one´s personality, thus burning one´s privacy to the ground.

Identity thieves (true personality surrogates) subtract a fraction of one´s unique and unrepeatable personality every time they use a false identity in the digital society.

In this light, privacy harm is not only objective and absolute but also a multiplied one: the more the personality surrogate (identity thief) uses a false identity further to a data breach, the more tainted will be one´s right to informational self-determination. Eventually, identity thieves will wipe out one´s core of undeniable and exclusive personhood from the face of digital society.

Here lies the real danger: data breaches indeed create a distressing backlash on citizens. But that is hardly the point. No matter how unsettling may be to perceive one´s personal data floating without hindrance in the «open market» of data brokerage, the real harm (meaning privacy harm) is an objective, multiplied and absolute one: the loss of chance of exclusive control of one´s personal data. The undeniable right of exclusive control of one´s personal data is indistinguishably connected with the right of free development of one´s personality in the realm of digital society we live in.

Right of free development of one´s personality encompasses a two-folded level of privacy that ought not to be taken away from citizen´s grasp: thematic privacy and spatial privacy. Both pertain to citizen´s quintessence that is not to be corrupted by misappropriation and misuse of personal data. Both appertain to that universe of exclusivity that citizens should be able to control at any cost. Citizens must be given the inarguable right to control to whom, when, what, how, and to what ends they disclose their personal data. Moreover, citizens must get to choose when they withdraw their consent to disclose their personal data, the kernel of their right of free development of one´s personality.

Why thematic privacy and spatial privacy are so important to preserve one´s right of free development of personality? [200].

Closely following the lesson of the German Constitutional Court (*Bundesverfassungsgericht–BVerfGE*), the *thematic privacy* comprises the very same universe covered by *privacy in a material sense*. Thematic privacy refers to an array personal data or personal realities that the holder of the natural right of privacy intend to subtract to the curiosity and to the public discussions [131,201], such as sexuality, deviant behaviours and diseases [202,203].

On the other hand, the *sphere of privacy in a spatial sense* belongs to an area of entrenchment of the individual that ensures the possibility of meeting and being with himself [204] and of evasion from the rest of digital society [205,206].

Meaning that there is an unreachable core of privacy that emerges from personal data of the citizens [207] that involves – and identifies with – the universe of things, facts, events, experiences, emotions, and places that covers fringes of irreducible subjectivity, individuality and personality [208,209], which the citizen legitimately intends to keep to himself and for a small number of «others» [210], therefore being that a space of guardianship of privacy, converted into a place of fulfillment of private life [211,212].

In this light, misappropriation and misuse of citizens´ personal data further to a data breach configures a «*big profligate*» (*grosser Lauschangriff*) [213-216], as they enshrine the ultimate loss of exclusive

control of one´s personal data.

Controlling and vesting others to gain access to personal data are manifestations of the right of free development of one´s personality [217]. Whenever unauthorized parties (identity thieves or similar people) glean unauthorized personal data, an objective, absolute and multiple harm of loss of chance of exclusive control of one´s personal data emerges in the digital society.

Being an objective, absolute and multiple harm, privacy harm arisen on the scope of data breach cases ought to be regarded as loss of chance of exclusive control of one´s personal data emerges in the digital society.

In regard of Article III Standing, U.S. Courts insist that data-breach harms be deep-rooted, ostensive, visceral, tangible [218] fairly easy to appraise [219], gauge, and quantify [220]. «They require harms to be vested—already materialized in the here and now. Plaintiffs must experience physical, monetary, or property damage or, at least, the damage must be imminent» [221].

For that reason, «most courts consider plaintiffs' fear, anxiety, and psychic distress about their increased risk of identity theft and other abuses too remote to warrant recognition» [222].

One tend to agree with this jurisprudential vein. Being too diffuse, the risk of identity theft [222,223] does not warrants immediate recognition. Rather, data breach itself does. Data breach is an early stage of a cognizable privacy harm. A tangible («injury in fact») privacy harm of loss of chance of exclusive control of one´s personal data arises from the data breach itself. Eventually, privacy harm of loss of chance of exclusive control of one´s personal data ought to give rise to standing.

Plaintiffs 'fear, anxiety, physical and emotional distress [224] about their heightened risk of identity theft are subjective backlashes which can warrant a larger or thinner compensation. They are not the privacy harm itself. Plaintiffs 'fear, anxiety, physical and emotional distress are a subjective repercussion of a privacy harm - loss of chance of exclusive control of one´s personal data arisen from a data breach, a concrete [225,226], autonomous [227-229], and tangible [230-232] harm.

Loss of chance of exclusive control of one´s personal data arisen from a data breach is an «injury in fact», thus allowing Article III Standing in data breaches cases.

Conclusions

Not long ago, Professor Jack Balkin asserted that humankind had surpassed the threshold of the «Pretty Good Privacy» (PGP). In his insightful view, we (humankind) currently live in a so-called «National Surveillance State», in which the core of our natural rights (such as privacy, preservation of one´s self-image, and undeniable «right to be left alone») are being progressively eroded. Privacy, «right to be left alone» and «reasonable expectation of privacy» are increasingly becoming a glimpse of the past, as the «analogic society» steadfastly faded away.

Swiftly heading towards an overarching «global-digital society», humankind faces candent challenges which rests upon the following conundrum: how to ascertain the boundaries of the murky circuit of Big data controlled by *surveillance intermediaries* (Facebook, Microsoft, Google, Ebay, Twitter, Yahoo!, We Chat, Apple)? In cases of data breaches, have citizens the right to seek redress from fiduciary data holders? If so, in what grounds? These questions are currently pressing in European Union, mainly from *data protection* and *cloud computing* standpoint.

In our assessment, data breaches should not prevent consumers (by definition, all of us) from seeking appropriate compensation from identified enterprises who were fiduciary holders of their personal data. The reason for this axiom rests upon a *natural right* to not only gain access to fragments of their individuality, subjectivity and intimacy (in short, personal data), but uttermost the *natural right to control* the *universe of personhood* deeply ingrained in their personal data.

Consumers or citizens ought to be given the natural right to choose when, how, to whom, and to what purposes their personal data can be disclosed to third parties. Conversely, in the wake of data breaches, consumers ought to be given the right to seek compensation from fiduciary data holders. That is paramount as for constituting a stronghold that protects consumers from the lingering perils of the digital society we live in.

Privacy ought to be regarded as citizens´ natural right. This approach stretches far beyond the mere juxtaposition between privacy and fundamental rights. Fundamental rights are mainly awarded within the scope of a Constitution. Fundamental rights boundaries arise from a document endorsed by a given electoral majority in a given historical moment. Fundamental rights are document-borne rights.

Antithetically, in our view, natural rights (for instance, privacy in the digital society in which we live in) are person-borne rights. Natural rights precede fundamental rights. As a result, natural rights are not a grotesque product of a capacious (or narrow) generosity of an array of lawmakers or legislators in a given historical time frame. Natural rights (such as privacy) do not depend on the circumstantial endorsement of lawmakers or legislators.

Natural rights are grains of personhood. Natural rights (such as privacy) erupt on digital society whenever a person born. Natural rights are particles of citizen's undeniable and unique subjectivity that Constitutions (let alone laws) ought to be unable to tear apart. Data breaches dissolves those seeds of citizen´s unique and unrepeatable personhood.

Digital society brought along a multitude of benefits to humankind, but that wide range of social prosperity cannot tarnish or squander citizens´ unique personhood every time a data breaches surfaces. Conversely, citizen´s ought to be able to seek redress or compensation whenever a data breach occurs.

Although originally a natural and human right, privacy can also be seen through the lens of a fundamental right. However, at the time of the enactment of U.S. Constitution privacy had a glaringly different scope and range when compared to 2018, a vivid receptacle of digital society. Privacy harkens back pre-internet era, but arguably did not encompass a wide range of perils associated to the then inexistent digital and computerized society we live in.

Accordingly, what a thin theory excludes from original public meaning of privacy is the original expected application of the text-how people at the time of adoption of U.S. Constitution would have expected that the text (enshrining right of privacy) would be applied to concrete situations, as in the pre-internet era massive data breaches occurred on the realm of digital society were definitely not an issue (let alone a major one) back then.

One can foresee that original public meaning of privacy does vary over time. This is paramount if one endeavors to ascertain the boundaries of privacy in the pre-internet era and of digital society we live in.

Original public meaning of privacy in the pre-internet era had a distinctively different scope if squarely compared to 2018. Protection of privacy in the pre-internet era had conspicuously dissimilar boundaries and a markedly narrower scope. Pre-internet era and analogic age have provided humankind the very last scent of a nearly-unshakable privacy. Concerns about privacy (though existent) were not pressing.

Protection of privacy in 2018 is a rather pressing issue amid intrusive government surveillance on the brave new world of digital society. Pervasive government surveillance seemingly has no bounds. Protection of privacy appears to be intertwined with an *overlapping consensus* that enshrouds the axiom that an unassailable right to be left alone in the digital society is not a moral conception, but a conception of justice.

A conception of justice (for privacy) is currently more pressing than ever before, especially in light of atrocious events (9/11), which have pushed the core of our natural, human and fundamental right of privacy to nearly-hollow standards, giving rise to the so-called «National Surveillance State». «National Surveillance State» is the original public meaning of privacy in 2018.

«National Surveillance State» is an expression coined by renowned doctrine a decade ago. This expression stems from a rather polymath approach: the world has changed dramatically since 9/11 events.

Prior to the unfortunate events that have taken place in 9/11, liberty and privacy (though subject to restrictions) were seemingly bullet-proof rights. Closely regarded as airtight rights. 9/11 brought along an atmosphere of unbearable suspicion, which has given rise to a widespread suppression of liberties and rights. Being discernably close to a far-reaching paranoia arisen from those hapless events, privacy has been caught on the middle of a callous and often ferocious battle between safeguarding security and harboring some civil rights.

In the aftermath of 9/11 events, balancing or squarely aligning those conflicting rights is a rather herculean task. No surprise stems from the fact that overall governments have chosen to confer priority to security, often wrapped under the seeming (yet real?) cloak of «public common good». As a result, privacy´s core has been severely weakened to historical minimum standards.

This abhorrent trend has been shrewdly portrayed by acclaimed doctrine. Ranging from intercepting phone calls in real time to capturing footage amid a rather oppressive surveillance, governments have conspicuously interfered on the core of citizen´s liberties and rights worldwide.

The «brave new world» of digital society, constituted by a remarkable electronic and technologic apparatus, has somehow heightened the degree of intrusion on citizen´s private sphere.

When it comes to pursuing the so-called «national security», or in a more polished manner «greater good», governments seem to have no restrictions whatsoever in order to accomplish the goal of security, as citizen´s personal data is being captured, stored, and processed (sometimes for abstruse and spurious ends) at an alarming rate with little regard for surveillance transparency. Digital society is seemingly governments' «tip of the spear» when it comes to «getting things done» swiftly and in a purely veiled manner: they see you and yet you don't see them.

To the extent governments perform invasive surveillance programs that corrodes citizen´s privacy, the degree of ubiquity of these technology-enabled surveillance tools heightens at the very same pace that governments bestows a duty of collection, storage, processing and dissemination of information (that is to say citizen´s personal data) to private parties placed on the second level of National Surveillance State. Governments expect full and unrestricted cooperation from selected private parties, in regard of capturing and disclosing citizens´ pertinent personal data. Most of the times (if not always) governments do get that fully expected cooperation.

A concrete danger surfaces on the third level of National Surveillance State when a strategic misalignment between Surveillance intermediaries or online intermediaries («quasi-governmental actors» or, to some extent, «corporate avatars») and governments occurs though. Worse yet, when online intermediaries adopt a belligerent and rather contentious vein against governments in the era of Internet of Things.

This brings us to the third layer of National Surveillance State: unlike the second level of National Surveillance State, in which private parties aid governments to pursuing condoned ends of collecting information to prevent terrorist attacks, surveillance intermediaries or online intermediaries somehow constrain the accomplishment of those ends by concealing crucial information from governments.

On the third layer of National Surveillance State, the erosion of privacy boundaries is far more damaging to citizen´s right of informational self-determination, as the unavailability to gain access to the batch of information withheld by surveillance intermediaries will only give rise to more government surveillance, thus corroding even further citizens 'privacy and opening a «new age of threats».

Simply do the math: more surveillance corresponds symmetrically to less privacy. In the process, so much for the tradeoff security-privacy, as (even) more government surveillance ought to override privacy´s minimum standards in the long-term.

This stems from the axiom that not only Surveillance intermediaries activities' lack regulatory oversight, but mainly due to the fact that governments are clueless about the extension of surveillance undertaken by online intermediaries. In short, this three-folded or multilayered National Surveillance State is potentially disruptive for citizens 'privacy as both governments and citizens are unaware of the depth and range of surveillance programs performed by online intermediaries.

Currently, this murkiness has given rise to a declared battle between governments and surveillance intermediaries over the control of personal data collected in electronic portable devices, such as IPhones: Apple´s high profile 2016 legal battle in which the company frantically challenged a court order «commanding it to help unlock the iPhone of one of the San Bernardino terrorists», portrays how central the question of regulating government surveillance has become in United States of America´s politics and law.

Make no mistake: when it comes to capturing, storing, withholding and mostly controlling citizens 'personal data, Surveillance intermediaries (who carries out proper «corporate surveillance») hold a sizable power. That power is not restricted to that though. Championing for civil rights (such as privacy) is becoming increasingly trendy amongst surveillance intermediaries, «as Verizon, which owns Yahoo, signed on to an amicus brief on behalf of leading tech companies in the pending Supreme Court case *Carpenter v. United States*, arguing that the Court should extend Fourth Amendment protections to geolocation data».

Surveillance intermediaries´ substantial power brings along an immediate danger: the interplay between «government surveillance»

and «corporate surveillance» can be often counterproductive and even more damaging to citizens ´ privacy: «at the first stage, surveillance intermediaries can help society better construct *surveillance frontiers*—menus of surveillance policy options—by adding more information and more diverse perspectives, as well as by minimizing inefficient alternatives. But they can also create negative second order effects by forcing the government to engage in more intrusive surveillance and by making it easier for the surveillance intermediaries themselves to collect more data on their users».

Being an axiom that Surveillance intermediaries hold a rather robust power, which enables them to constrain government´s surveillance agenda, question is to fathom its real depth and extent or, more prosaically, «how» and «when» they exercise this power.

A surveillance intermediary is typically a party that collects massive tons of sensitive information, customarily for its own business purposes, that the government wants—for example, phone company billing records that contain a cellphone subscriber's call history background. Instead of delving information from the target directly (specified agglomeration of citizens or persons of interest in a given criminal investigation), the government seeks it from the third party, either because it's far easier to get the information that way or because only the third party has the information. The third party becomes a *surveillance intermediary*: it stands squarely between the government and the target of the surveillance.

As a result, government surveillance and corporate surveillance (truly middlemen or gatekeepers) creates multiple layers of surveillance in which every side conceal information from each other and, worse, with limited or inexistent regulatory oversight.

Digital society and Multilayered National Surveillance State, especially at the third level, stands at crossroads: should societal interest in granting national security through security surveillance supersede protection of privacy by enabling governments to gaining access to encrypted systems? Antithetically, should surveillance intermediaries continue to opposing certain forms of government surveillance «employing default encryption technologies on mobile devices and explicitly marketing them as being impervious to government snooping»?

Concretely, how can one manage to strike a balance between societal interests in chasing «bad guys», pursued by government's law enforcement agencies, with the egoistical interests pursed by mighty corporations or surveillance intermediaries? On the previously asserted cases of strategical misalignment between law enforcement government agencies and multinational corporations (just like the one occurred in San Bernardino terrorist attacks), one should refer to the prototypal principles of proportionality and human dignity.

Throughout this manuscript I have been championing for protection of citizens´ privacy from governments´ prying eyes. A vigorous defense for security concerns is seemingly contradictory at that glance. A cautious note comes in handy: one should not forsake that privacy cannot always prevail over security at any cost.

One should bear in mind that sometimes too much privacy can be as equivalent as opening the Pandora box of perennial insecurity with deleterious effects on the long-term common good – bullet-proof privacy can pave the way to even more vicious terrorist attacks which will give rise to an ever-present security, thus pushing privacy to a tokenistic value or inexistent one at all.

Striking a delicate balance between principle of security and principles of proportionality and his «companion route» principle of human dignity is definitely a challenge that one should embrace. How can one accomplish such an arduous task? Displaying the pivotal value of principle of proportionality coupled with the seminal principle of human dignity.

Principle of proportionality, which in recent decades achieved remarkable recognition in theory and practice of the control of constitutionality consists of three subprinciples: adequacy, necessity and the proportionality in a strict sense.

These three lines express the idea of optimization, a precious asset when it comes to balancing seemingly conflicting principles or, in a broader sense, opposing interests, such as the ones pursued by law enforcement government agencies and surveillance intermediaries.

Conflicting principles (impervious security and privacy, inextricably linked with the principle of human dignity), require a constant optimization in relation to what is factual e legally possible.

Subprinciples of adequacy and of necessity refer to the optimization concerning the existent factual possibilities (gathering information from surveillance intermediaries pertaining to a criminal event) – on our lens, it suits perfectly in the sphere of surveillance intermediaries the share of information with government agencies of law enforcement, for purposes of prevention and repression of terrorist attacks provided that the sharing of that information is restricted to personal data solely related with criminal events. From that point onward, principle of security ought to submerge and the principle of human dignity (which wraps the inner and outer limits of privacy) ought to emerge at his maximum height.

United States Supreme Court and Federal Courts set out insurmountable high standards in regard of Article III Standing in Surveillance cases, thus hindering the success rate of claims in which plaintiffs (citizens/consumers) sought appropriate redress from the government.

The very same insurmountable high standards in regard of Article III Standing have been transferred to data breach cases. Just take a look of what is happening on the scope of federal class actions. This issue is not a small one. The burgeoning digitalization of our personal data has created corresponding increase in the bulk of electronically stored private information in the domain of third parties.

That private information is at risk of theft, loss, or manipulation by unidentified third parties, generally hackers, whose intentions are far from being merely angelical. When hackers attack and subtract citizen's personal data, «victims often band together in federal class actions, naming the custodians of their private data as defendants».

However, «district courts are dismissing these class action claims at the doorstep for lack of Article III standing. The corporate defendants argue, and many courts agree, that a plaintiff's alleged increased risk of future data misappropriation is insufficient to satisfy the U.S. Supreme Court's test for an "injury in fact," a critical component of the traditional standing analysis».

Privacy harm is not an intangible and far-fetched injury. Anxiety and unsureness as to whether personal data is going to be used in the future to the practice of misdeeds are an ulterior consequence of a data breach. Anxiety and unsureness are a subjective backlash of a data breach. They are not the privacy harm itself.

Anxiety and unsureness being an inward state are hardly the harm

itself. Anxiety and unsureness are not palpable and cognizable at a judge´s lens. Quite the opposite, privacy harm is related with the free development of one´s personality in an objective sense. Every time a data breach occurs a fragment of one´s eminent and unique personhood is besmeared. Privacy harm consists of that subtraction of one´s unique and unrepeatable personhood. That unrepeatable personhood deeply ingrained in citizens´ personal data is objective and absolute. There is no such thing as repeated personalities or repeated personhoods.

Privacy harm is objective because it is centered on the unique and absolute nature of one´s eminent personhood. Privacy harm is absolute because the personal data subtracted further a data breach belongs to a zone of exclusivity that no one should be allowed to interfere but the aggrieved citizen. The aggrieved citizen has the exclusive control of fragments of his undeniable, unique and absolute personhood.

This approach is squarely aligned with our starting point: privacy is a natural right. Privacy is a human right. Privacy is not (just) a fundamental right, always dependent on occasional or seasonal lawmakers 'good mood.

Being a natural right, privacy is inextricably linked with the objective and absolute value of human being. Personal data (thus privacy) are fragments of a one-of-a-kind human being that is not to be smeared, let alone in an unauthorized manner.

Identity theft constitutes a striking example of how an identity thief can begrime one´s unique and absolute personhood.

Identity theft cases are the hallmark of personality debasement. Every identity theft case has a stereotyped feature: identity thieves endeavor to erase a unique personality from digital society with *multiple shots*. Make no mistake: identity theft cases can produce a staggering amount of damage on the free development of one´s personality, thus burning one´s privacy to the ground.

Identity thieves (true personality surrogates) subtract a fraction of one´s unique and unrepeatable personality every time they use a false identity in the digital society.

In this light, privacy harm is not only objective and absolute but also a *multiplied* one: the more the personality surrogate (identity thief) uses a false identity further to a data breach, the more tainted will be one´s right to informational self-determination. Eventually, identity thieves will wipe out one´s core of undeniable and exclusive personhood from the face of digital society.

Here lies the real danger: data breaches indeed create a distressing backlash on citizens. But that is hardly the point. No matter how unsettling may be to perceive one´s personal data floating without hindrance in the «open market» of data brokerage, the real harm (meaning privacy harm) is an *objective*, *multiplied* and *absolute* one: the loss of chance of exclusive control of one´s personal data. The undeniable right of exclusive control of one´s personal data is indistinguishably connected with the right of free development of one´s personality in the realm of digital society we live in.

Right of free development of one´s personality encompasses a two-folded level of privacy that ought not to be taken away from citizen´s grasp: *thematic privacy* and *spatial privacy*. Both pertain to citizen´s quintessence that is not to be corrupted by misappropriation and misuse of personal data. Both appertain to that universe of exclusivity that citizens should be able to *control* at any cost.

Citizens must be given the inarguable right to control to whom, when, what, how, and to what ends they disclose their personal data. Moreover, citizens must get to choose when they withdraw their consent to disclose their personal data, the kernel of their right of free development of one´s personality.

Plaintiffs 'fear, anxiety, physical and emotional distress are a subjective repercussion of a privacy harm - loss of chance of exclusive control of one´s personal data arisen from a data breach, a concrete, autonomous, and tangible harm.

Loss of chance of exclusive control of one´s personal data arisen from a data breach is an «injury in fact», thus allowing Article III Standing in data breaches cases.

References

1. Calo MR (2010) People can be so fake: A new dimension to privacy and technology scholarship. Penn State Law Review 114: 809, 842–48.
2. Andrade MC (2012) The criminal protection of image in germany and portugal. Journal of Legislation and Jurisprudence 141: 143-144.
3. Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419, 433 (1982).
4. Strahilevitz L (2008) Reputation nation: law in an era of ubiquitous personal information. Northwestern University Law Review 102: 1667.
5. Ribeiro JS (2013) The guardian of personal property in the portuguese constitutional constitution and jurisprudence. Studies of Homage to Prof. Doctor Jose Joaquim Gomes Canotilho, p: 853.
6. European Court of Human Rights, Copland v. United Kingdom, 3/4/2007.
7. Gonzalez F, Gloria R (2012) The fundamental right of data protection in the european union: in search for an uncharted right. International Review of Law, Computer & Technology 26: 3-10.
8. Kuan WH, J Horne J, Millard C (2012) Data protection jurisdiction and cloud computing when are cloud users and providers subject to EU data protection law the cloud of unknowing. International Review of Law, Computer & Technology 26: 129-169.
9. Campbell J (2017) Natural rights and the first amendment. The Yale Law Journal 127: 246-322.
10. Nat'l Cable & Telecomms. Ass'n v. Fed. Commc'ns Comm'n, 555 F.3d 996, 1001 (D.C. Cir. 2009).
11. Engels S, Jurgens U (2007) Effects of the ECHR right to privacy. possibilities and limits of the implementation of the "Caroline"-Urteis in German Law ". New Juristisches Wochenschrift, p: 2520.
12. Schwartz PA (2000) Commentary, internet privacy and the state. Connecticut Law Review 32: 820.
13. Meyler B (2006) Towards a common law originalism. Stanford Law Review 59: 551-581.
14. Campbell j (2017) Natural rights and the first amendment. The Yale Law Journal 127: 252.
15. Bickford CB (1992) Documentary history of the first federal congress of the united states of america. Congressional Debates 11: 811-822.
16. Richmond R (1788) The impartial examiner 1, Va.Indep.Chron.
17. Campbell J (2017) Republicanism and natural rights at the founding. Constitutional Commentary 32: 85-87.
18. Klement JH (2008) Of benefit of a theory that explains everything. Lawyer Newspaper 63: 756-763.
19. Jestaedt M (2007) The theory of contemplation its strengths and its weaknesses. Festschrift for Iseensee, pp: 260-268.
20. Alexy R (2006) Discourse theory and fundamental rights. Arguing Fundamental Rights, pp: 15-29.
21. Alexy R (2010) Fundamental rights. Encyclopaedia Philosophy 1: 950.
22. Alexy R (2011) Fundamental rights and proportionality". In: Utz Schliesky, Christian Ernst, Sönke Schulz (eds.) The freedom of man in the commune, state and Europe. Festschrift for Edzard Schmidt-Jortzig, pp: 3-15.
23. Balkin JM (2016) The construction of public original meaning. Constitutional

Commentary 26: 78.

24. Balkin JM (2013) Must we be faithful to original meaning. Jerusalem Review Legal Study 7: 57-77.
25. Rakovc JN (2011) Joe the ploughman reads the constitution, or, the poverty of public meaning originalism. San Diego Law Review 48:1-575.
26. Alexy R (1998) The institutionalization of human rights in the democratic constitutional state. Philosophy of Human Rights, pp: 246-254.
27. Balkin JM (2013) "The new originalism and the uses of history". Fordham Law Review 82: 641-646.
28. Cornell S (2014) Conflict, consensus & constitutional meaning: The enduring legacy of charles beard. Constitutional Commentary 3: 383.
29. Volokh E (2009) Symbolic expression and the original meaning of the first amendment. George Washington Law Journal 97: 1057, 1079-1083.
30. Green CR (2006) Originalism and the sense-reference distinction. Saint Louis University Law Journal 50: 555-559.
31. Smolla RA (2016) Smolla and nimmer on freedom of speech, pp: 1-11.
32. Whittington KE (2013) Originalism: A critical introduction. Fordham Law Review 82: 375-383.
33. Kent A (2013)The New originalism and the foreign affairs constitution. Fordham Law Review 82 : 758-759.
34. Whittington KE (2004) The new originalism. Georgetown Journal of Law & Public Policy 22: 599-613.
35. Solum LB (2009) District of columbia v. heller and originalism. Northwestern University Law Review, pp: 918-924.
36. Balkin J (2011) Living originalism. Harvard University Press, pp:1-480.
37. Colby TB (2011) The sacrifice of the new originalism. Georgetown Law Journal 99: 709-718.
38. Barnett RE (2013) Restoring the lost constitution. The Presumption of Liberty, p: 18.
39. Berman MN (2009) Originalism is bunk. New York Law Review 84: 1-8.
40. John Rawls (1999) A theory of justice, p: 340.
41. Dworkin R (1986) Law´s empire,p: 239.
42. Donnan M (2014) Rawl´s notion of overlapping consensus, p: 1.
43. Rawls J (1993) Political liberalism, pp: 34–49.
44. Balkin JM (2016) The construction of public original meaning. Constitutional Commentary, p: 80.
45. Dworkin R(1986) Law´s Empire, p: 242.
46. United States v. Jones (2012) Us supreme court. Legal Information Institute.
47. Donnan M (2014) Rawl´s notion of overlapping consensus, p: 3.
48. Rawls J (1987) The idea of an overlapping consensus. Oxford J Legal Studies 7: 1-25.
49. Rawls J (1955) Two concepts of rules. The Philoso Rev, p: 3.
50. Adam Smith (1759) The theory of moral sentiments, pp: 5-13.
51. Arneson R (2016) Joel feinberg and the Justification of hard paternalism, p: 1.
52. Feinberg J (1984) Harm to others, p: 23.
53. Mill JS (197) On liberty: critical essays.
54. Hart HL (1959) Concept of law, p: 86.
55. Alexy R (2002) The argument from the Injustice, p: 5.
56. Balkin J (2008) "Constitution in the national surveillance state". Minnesota Law Review 93: 1.
57. United States v. U.S. District Court (Keith) (1972) 407 U.S. 297, 314.
58. Solove DJ (2011) Nothing to hide: The false tradeoff between privacy and security (introduction), Yale University Press, pp: 1-2.
59. Manes J (2016) Online service providers and surveillance law transparency. Yale Law Journal 125: 343-351.
60. Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003).
61. Balkin J (2008) "Constitution in the national surveillance state". Minnesota Law Review 93: 2.
62. Balkin J (2008) "Constitution in the national surveillance state". Minnesota Law Review, 93: 3.
63. Calo R (2016) Can americans resist surveillance. The University of Chicago Law Rev 83: 24.
64. Michaels DJ (2008) All the president's spies: private-public intelligence partnerships in the war on terror. California Law Rev 96: 901-928.
65. Kohl U (2011) The rise and rise of online intermediaries in the governance of the internet and beyond- Connectivity intermediaries. Intern Rev Law Com Technol 26: 1.
66. Solove DJ (2014) The FTC and the new common law of privacy. Columbia Law Rev 114: 683-765.
67. Teubner G (2012) Alternative commentary to the civil gezetzbuch, pp: 1-6.
68. Solove D (2006) Taxonomy of privacy. University of Pennsylvania Law Rev 154: 519-520.
69. Banks WC (2010) Programmatic surveillance and FISA: of needles in haystacks. Texas Law Rev 88: 1633- 1637.
70. Koren NE, Haber E (2016) Governance by proxy: cyber challenges to civil liberties. Brooklyn Law Rev 82: 143-144.
71. Hobbes T (2012) Leviathan, with selected variants from the Latin edition of 1668 (Hackett Classics), p: 8.
72. 50 U.S.C. § 1881 (2012).
73. Donohue LK (2015) Section 702 and the collection of international telephone and internet conten. Harv JL Pub Poly 117: 43.
74. Standing, surveillance, and technology companies (2018) Harvard Law Review 131: 1742-1745.
75. Daskal J (2015) The un-territoriality of data. Yale Law J 125: 388-397.
76. Woods AK (2016) Against data exceptionalism. Stanford Law Rev 68: 738-751.
77. Solove DJ (2002) Digital dossiers and the dissipation of fourth amendment privacy. California Law Rev 75: 1083-1100.
78. Donohue LK (2016) The future of foreign intelligence: privacy and surveillance in a digital age, pp: 54-55.
79. Corn GS (2015) Essay, averting the inherent dangers of going dark: why congress must require a locked front door to encrypted data. Washington Lee Law Rev 72: 1433-1437.
80. Solove DJ (2011) Nothing to hide: the false trade off between privacy and security, pp: 101-110.
81. Schwartz PM (2011) PII Problem: privacy and a new concept of personally identifiable information. New York Law Rev 86: 1836-1892.
82. Rowell A (2012) Partial valuation in cost-benefit analysis. Adm Law Rev 64: 723-734.
83. Livermore M (2011) A brief comment on humanizing cost-benefit analysis. Eur J Risk Reg 13: 101.
84. Bayefsky R (2014) Dignity as a value in agency cost-benefit analysis. Yale Law J 123: 1732.
85. Rao N (2012) American dignity and healthcare reform. Harvard Law Rev 35: 171, 178-179.
86. Sunstein CR (2015) Financial regulation and cost-benefits analysis. Yale Law Journal 124: 272.
87. Gordon J (2014) The Empty call for cost-benefits analysis for financial regulators. Journal of Legal Studies 43: 351.
88. Sunstein CR (2014) The limits of quantification. California Law Review 102: 1369.
89. Adler M, Posner EA (2006) New foundations of cost-benefit analysis. Regulation and Governance 3: 72.

90. Miles TJ, Sunstein CR (2008) The real world of arbitrariness review. University of Chicago Law Review 75: 761.

91. Coates JC (2015) Cost-benefit analysis of financial regulation: case studies and implications. Yale Law Journal 124: 882-1345.

92. Posner EA, Weyl EG (2015) Cost-benefit analysis of financial regulations: response to criticisms. Yale Law Journal 124: 246-265.

93. Sunstein CR (2014) Valuing life: humanizing the regulatory state. The University of Chicago Press Books, pp: 1-240.

94. Klein A, Christian M, Olsen M, Campos T (2017) The "Section 702" Surveillance program. Ctr, New AM. Security.

95. Slobogin C (2014) Panvasive surveillance, political process theory, and the nondelegation doctrine. Georgetown Law Journal 102: 1721-1725.

96. Savage C (2015) Power wars: Inside obama´s Post-9/11 Presidency. Congress and Presidency 43: 262-264.

97. Wu T (2010) The Master Switch: The Rise and Fall of Information Empires. Business and Economics, pp: 1-366.

98. Risen J, Lichtblau E (2005) Bush lets U.S. spy on callers without courts. New York Times.

99. Balkin JM (2014) Old-school/new-school speech regulation. Harvard Law Review 127: 2296-2298.

100. Kim SN, Telman DAJ (2015) Internet giants as quasi-governmental actors and the limits of contractual Consent. Missouri Law Review 80: 723.

101. Avidan Y (2015) Corporate avatars and the erosion of the populist fourth amendment. Iowa Law Review 100: 1444-1458.

102. Benner K, Lichtblau E (2016) U.S. says it has unlocked iPhone without apple, New York Times.

103. Berman M, Zapotosky M (2016) The FBI paid more than $1 million to crack the san bernardino iPhone. The Washington Post.

104. Ferguson AG (2016) The internet of things and the fourth amendment of effects. California Law Review 104: 805-808.

105. Schneier B (2015) Data and goliath: the hidden battles to collect your data and control your world, pp: 207-210.

106. Informationelle Selbstbestimmung, ruling of german constitutional court (BVerfGE).

107. Wittes B, Blum G (2015) The Future of violence: robots and germs, hackers and drones; confronting a new age of threat. Terrorism and Political Violence, pp: 123-148.

108. Pozen DE (2016) Privacy-privacy tradeoffs. University of Chicago Law Review 83: 221-222.

109. Hare S (2016) For your eyes only: U.S. technology companies, sovereign states, and the battle over data protection. Bus Horizons 59: 549-561.

110. Rozenshtein AZ (2018) Surveillance intermediaries. Stanford Law Review 70: 99-102.

111. Kris D (2016) Trends and predictions in foreign intelligence surveillance: The FAA and beyond. Journal of National Security and Policy 8: 377-408.

112. Harcourt BE (2015) Exposed: desire and disobedience in the digital age 79.

113. Carpenter V (2017) Brief for technology companies as amici curiae in support of neither party at 8-9, 29-32, United States.

114. Rozenshtein AZ (2018) Surveillance intermediaries. Stanford Law Review 70: 110-117.

115. Rozenshtein AZ (2018) Surveillance intermediaries. Stanford Law Review 70: 110.

116. Rozenshtein AZ (2018) Surveillance intermediaries", Stanford Law Review 70: 112.

117. Rozenshtein AZ (2018) Surveillance intermediaries", Stanford Law Review 70: 115.

118. Sanchez J (2014) Snowden showed us just how big the panopticon really was. Now it's up to us.

119. One should not forsake Zuckerberg´s answer to an U.S. Senator amid facebook´s U.S. senate hearing held in 11/04/2018.

120. Rozenshtein AZ (2018) Surveillance intermediaries. Stanford Law Review 70: 117.

121. Kim NS, Telman DA (2015) Internet giants as quasi-governmental actors and the limits of contractual consent 80: 745.

122. Calo R (2014) Digital market manipulation, George Washington Law Review, pp: 999-1051.

123. Abelson H, Anderson R, Bellovin SM, Benaloh J, Blaze M, et al. (2015) Computer science & artificial intelligence laboratory technical report. MIT-CSAIL-TR-2015-026.

124. Renan D (2016) The fourth amendment as administrative governance. Stanford Law Review 68: 1039- 1127.

125. Swire P, Ahmad K (2012) Encryption and globalization. Columbia science and technology law review 13: 418-420.

126. Rascoff SJ (2016) Presidential intelligence. Harvard Law Review 129: 662-665.

127. Calo R (2011) The boundaries of privacy harm, 86 Indiana Law Journal: 1137: note 29.

128. Posner RA (2008) Privacy, surveillance, and law. University of Chicago Law School 75: 251.

129. Stuntz WJ (2006) Secret service: against privacy and transparency. New Republic.

130. Barak A (2012) Proportionality: constitutional Rights and their limitations, pp: 186-204.

131. Santos HLD (2015) A brave new world of ambient intelligence in the casinos of Macau: Reality or fiction?. UNLV Gaming Research and Review Journal 19: 1-4.

132. Stone A, Mathews J (2008) Proportionality balancing and global constitucionalism. Columbia Journal of Transnational Law 47: 72-164.

133. Beatty DM (2005) The ultimate rule of law. Oxford University Press, pp: 34-49.

134. Seidman LM (2012) Never mind the constitution, on constitution disobedience, New York, Oxford University, pp: 12-35.

135. Waldron J (2014) Book review never mind the constitution, on constitution disobedience. Harvard Law Review 127: 1147-1172.

136. Bochenforde EW (1991) Fundamental rights as basic norms. Frankfurt am Main, pp: 188-190.

137. Alexy R (2008) Theory of juristical argumentation. Frankfurt am Main, Suhrkamp, pp: 273-283.

138. Alexy R (2002) Theory of constitutional rights. Oxford University Press, pp: 47-49.

139. Helm SV (1983) 463, U.S. 277 (Assessing the proportionality of a sentence of life imprisonment).

140. Massachusetts PV (1867) 72 U.S. (5 Wall.) 475, 480.

141. Neil OV, Vermont (1892) 144 U.S. 323, 331.

142. Alexy R (2008) Theory of legal argumentation. The theory of rational discourse as a theory of legal justification, pp: 273-283.

143. Zagrebelsky G (2008) The constitutional judge in the 21st Century, Ibero. American Journal of Constitutional Procedural Law, p:248.

144. Guastini R (2005) The constitutionalization of the legal order: the Italian case, Madrid: Editorial Trotta, pp: 49-75.

145. Dworkin R (1982) Taking rights seriously, Duckworth Books, London, pp: 3-88.

146. Alexy R (2015) Fundamental rights and the principle of proportionality 146: 821.

147. Alexy R (2010) On the nature of legal principles. Archives for Philosophy of Law, Franz Steiner & Nomos 119: 9-18.

148. Alexy R (2002) Theory of constitutional rights. Oxford University Press, pp: 47-49.

149. Samuel A, Alito SA (2010) United States v. Stevens, 599 U.S, pp: 460- 470.

150. Alexy R (2007) The weight formula, frontiers of economics analysis of law-studies in the philosophy of law. Jagiellonian University Press 3: 9-27.

151. Dworkin R (1986) Law´s empire. oxford, portland, oregon. Hart Publishing, pp: 288-342, 403-418.

152. Alexy R (2003) On balancing and subsumption a structural comparison. Ratio Juris 16: 433-448.

153. Alexy R (1989) A theory of legal argumentation. Oxford, Claredon Press, pp: 221-230.

154. Jeanne P, Bonnici M (2012) Exploring the non-absolute nature of right of data protection. International Review of Law, Computer & Technology 28: 131-143.

155. Jackson VC (2015) "Constitutional law in an age of proportionality". Yale Law Journal 124: 3094-3114.

156. Graham V (2010) The concept of proportionality is central to the eight amendment. USCA Const Amend 8.

157. Heller V (2008) District of Columbia. 554 US 570.

158. United States v. Alvarez (2012) 132 S. Ct 2537.

159. Charkaoui v. Canada (2007) Citizenship and immigration. 1 S.C.R. 350, 2007 SCC 9.

160. Mounted Police Association of Ontario v. Canada (2015) Attorney General. 2015 SCC 1, 1 S.C.R. 3.

161. Hicks M, Ellis C (2018) The cambridge analytica and facebook data scandal: how to tell if your data was shared.

162. Balkin MJ (2008) Constitution in the national surveillance state. Minnesota Law Review 93:1-25.

163. Solove DJ (2004) The digital person: technology and privacy in the Information age, New York University Press, pp: 1-269.

164. Solove D (2013) Introduction: Privacy self-management and the consent dilemma. Harvard Law Review 126: 1888-1889.

165. Goldman E (2005) Data mining and attention consumption. Privacy and Technologies Identity, pp: 225-226.

166. Solove D (2006) Taxonomy of privacy. University of Pennsylvania Law Review 154: 490.

167. Canotilho G (2007) Privatization and rights, freedoms and guarantees. Regarding the secrecy of correspondence in the telecommunications service, Studies of Fundamental Rights, pp: 158-169.

168. Solove D (2006) Taxonomy of privacy. University of Pennsylvania Law Review 154: 519-520.

169. U.S. CONST. art. III, 2.

170. Zakharov V. Russia (2015) The european court of human rights, sitting as a grand chamber. ECHR, no. 47143/06.

171. Malone V (1984) Commissioner of the police for the metropolis.

172. Andrew R (2015) Privacy, data retention and domination: Digital rights ireland ltd v minister for communications. The Modern Law Review, pp: 535-548.

173. Volkerund Markus Schecke, process n. C-92/09 e C-93/09.

174. Solove DJ (2003) Identity theft, privacy, and the architecture of vulnerability. Hastings Law Journal 54: 1227-1232.

175. Lujan V (1992) Defenders of wildlife. Justia US Supreme Court 504 U.S. 555, pp: 560-561.

176. Spokeo, Inc. v. Robins (2016) 136 S. Ct. 1540, 1547.

177. Dana Post (2014) Plaintiffs alleging only future harm following a data breach continue to face a high bar. Int'l Ass'n of Privacy Prof'ls.

178. Chao DV (2004) Certiorari to the united states court of appeals for the fourth circuit. Justia US Supreme Court 540 U.S. 614.

179. Green N (2017) Standing in the future: the case for a substantial risk theory of Injury-in-fact in consumer data breach class actions. Boston Law Review 58: 292.

180. Hughes FV (1992) Appeal from the court of appeals of the district of columbia. US Supreme Court 258 U.S. 126.

181. Calo R (2011) The boundaries of privacy harm. Indiana Law Journal 86: 1145.

182. United States v. United States District Court (Keith) (1972) 407 U.S. 297: 314, 408-U.S. 1-11.

183. 408 U.S. 1, 11 (1972).

184. Miller AR (2009) Privacy: is there any left?. Federal Courts Law Review 3: 87-100.

185. Calo R (2011) The boundaries of privacy harm. Indiana Law Journal 86: 1146.

186. Green N (2017) Standing in the future: The case for a substantial risk theory of "Injury-in-Fact" in consumer data breach class actions. Boston Law Review 58: 287.

187. Clapper V (2012) Amnesty International. USA 28 U.S.C. 1332.

188. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).

189. Green N (2017) Standing in the future: The case for a substantial risk theory of "Injury-in-Fact" in consumer data breach class actions. Boston Law Review 58: 287-288.

190. Solove DJ (2008) The new vulnerability: data security and personal information. Securing Privacy in the Internet Age, pp: 111–112.

191. Exxon mobil corp. v. allapattah servs., Inc., 545 U.S. 546, 552 (2005).

192. Federal Rules of Civil Procedure 12(h)(3).

193. Nicholas G (2017) Standing in the future: the case for a substantial risk theory of "injury-in-fact" in consumer data breach class actions. Boston Law Review 58: 288.

194. Raines v. Byrd, 521 U.S. 811, 818 (1997).

195. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) confirming that standing is an "irreducible constitutional minimum.

196. Richie JT (2015) Data breach class actions, bus litig. Committee News l.

197. Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013). Plaintiffs have no standing to challange FISA because they cannot prove they were subject to surveillance.

198. Solove DJ, Citron DK (2017) Risk and anxiety: a theory of data breach arms. Texas Law Review 96: 737.

199. Calo R (2011) The boundaries of privacy harm. Indiana Law Journal 86: 1133-1134.

200. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).

201. Solove DJ, Citron DK (2018) Risk and anxiety: a theory of data breach arms. Texas Law Review 96: 763.

202. Ruling of the German constitutional court (2008) (Bundesverfassungsgerricht – BVerfGE), Neue Juristichen Wochenschrift, p: 1794.

203. Andrade MDC (2008) Domicile, intimacy and constitution. Journal of Legislation and Jurisprudence 138: 110.

204. Ruling of german constitutional court (2000) (Bundesverfassungsgerricht-BVerfGE), Neue Juristichen Wochenschrift, p: 1022.

205. Clifford T (2016) Provider liability and medical identity theft: can I get your (insurance) number?. Northwestern Journal of Law and Social Policy 12: 45-67.

206. Us Supreme Court, United States v. Jones, de 24/01/2012: (access: 14/04/2018) (about geolocation data provided by GPS tracking devices constitutes a striking example of spatial privacy in the realm of digital society).

207. German doctrine (2007) About the contraposition of the sphere of the thematic privacy/sphere of the spatial privacy. S Engels/U Jurgens, New Juristisches Wochenschrift, p: 2517.

208. Ruling of German Constitutional Court (2008) (Bundesverfassungsgerricht-BVerfGE), Neue Juristichen Wochenschrift, p: 1794.

209. Ruling of constitutional court of portugal, no. 403/2015.

210. Protection traffic data of communications is covered by the scope of protection of this fundamental right thus Ruling of 08/04/2014, Digital Rights Ireland Ltd., processes no. C-293/12 e C-594/12, that annulled directive 2004/26/CE, by violation of the articles 7 and 8 of the charter of fundamental rights.

211. Court of justice of european union (CJEU) referred that this right "is closely connected with the right to respect of private life" (Ruling of 09/11/2010, Volkerund Markus Schecke, process no. C-92/09 e C-93/09).

212. Ruling of the german constitutional court (BGHSt) (2006) 50: 206-216.

213. Malone V (1984) United kingdom referred that the access and use of data concerning traffic of communications is covered by the protection of no. 1 of ART 8 of the ECHR (Ruling of 02/08/1984, complaint no. 8691/79).

214. Böckenforde, in: Juristichen Zeitung (*JZ*), (2008): 926.

215. Ruling of german constitutional court (Federal Constitutional Court-BVerfGE) (2004) Neue Juristichen Wochenschrift , pp: 1000-1002.

216. The notion of grosser Lauschangriff was set again in the Ruling of German Constitutional Court (Bundesverfassungsgerricht – BVerfGE), known as Carolina II, Neue Juristichen Wochenschrift (2008): 1793

217. About this seminal jurisprudential decision, see, in the German doctrine, S. Engels/U. Jürgens, "Auswirkungen der EGMR-Rechts-prechung zum Privatsphärenschutz. Möglichkeiten und Grenzen der Umsetzung des "Caroline"–Urteis in deutschen Recht", *Neue Juristichen Wochenschrift* (2007): 2520.

218. BVerfGE (1973) 34, 238, "Juristichen Zeitung (JZ)", p: 505.

219. Sci applications int'l corp (SAIC) Backup tape data theft litig 45: 3d 14.

220. Amburgy (emphasizing that the "injury or threat of injury must be concrete and particularized, actual and imminent; not conjectural or hypothetical"). 671 F. Supp. 2d at 1050, 1053–1055.

221. Maglio V (2015) Advocate health and hosps. Corp, pp: 746-755.

222. Solove DJ, Citron DK (2018) Risk and anxiety: a theory of data breach harms. Texas Law Review 96: 752-754.

223. Solove DJ, Citron DK (2018) Risk and anxiety: a theory of data breach harms. Texas Law Review 96: 757.

224. Solove DJ, Citron DK (2018) Risk and anxiety: a theory of data breach harms. Texas Law Review 96: 756.

225. In German doctrine (2004) Gerald Masch, Chance und Schaden: zur Dienstleitsterhaftung bei unaufklärbaren Kausalverläufen, Tübingen, Mohr Siebeck,: 128 ff.

226. In Italian doctrine, Cristina Severi (2003) "Perdita di chance e danno patrimoniale risarcibile", RcP, LXVIII (2): 305 ff.

227. In German doctrine, Helmut Koziol (2007) "Schadenersatz für den Verlust einer Chance?", Festschrift für F. STOLL zum 75. Geburstag, Tübingen, Mohr Siebeck, pp: 233-250.

228. Nils Jansen (1999) "The idea of a lost chance", Oxford Journal of Legal Studies 19: 271-296.

229. In Spanish doctrine, Luis Medina Alcoz (2007) La teoria de la perdida de oportunidade. Estudio doctrinal y jurisprudencial de derecho de daños público y privado, Madrid, Civitas, p: 58 ff.

230. In French doctrine, Lois Raschel (2010) "La délicate distinction de la perte de chance et du risque du domamage". J.C.P, p: 763 ff.

231. In English doctrine, Mark Lunney/Ken Oliphant (2013) Tort Law: Text and Materials, Oxford, p: 208.

232. In Portuguese doctrine, Rui Cardona Ferreira (2017) "A perda de chance na responsabilidade civil por ato médico", Revista de Direito Civil, II 1: 131-155.