Preprint from http://rosariataddeo.net
This is a preprint version of an article accepted for publication in *Science and Engineering Ethics*.

The *struggle between liberties and authorities* in the information age

Mariarosaria Taddeo

Department of Politics and International Studies, University of Warwick

Abstract

The "*struggle between liberties and authorities*", as described by Mill, refers to the tension between individual rights and the rules restricting them that are imposed by public authorities exerting their power over civil society. In this paper I argue that contemporary information societies are experiencing a new form of such a struggle, which now involves liberties and authorities in the cyber-sphere and, more specifically, refers to the tension between cyber-security measures and individual liberties. Ethicists, political philosophers and political scientists have long debated how to strike an ethically sound balance between security measures and individual rights. I argue that such a balance can only be reached once individual rights are clearly defined, and that such a definition cannot prescind from an analysis of individual well-being in the information age. Hence, I propose an analysis of individual well-being which rests on the Capability Approach, and I then identify a set of rights that individuals should claim for themselves. Finally, I consider a criterion for balancing the proposed set of individual rights with cyber-security measures in the information age.

Keywords: Capability Approach, Cyber-security, Individual Rights, Levels of Abstraction, Online Persona, Well-being.

The *struggle between liberties and authorities* in the information age

1. Introduction

The "*struggle between liberties and authorities*", as described by Mill (Mill, 2002, p. 98), refers to the tension between individual rights and the rules restricting them that are imposed by public authorities exerting their power over civil society. The way in which the struggle is addressed determines the difference between pluralistic, democratic societies and authoritative ones, the former being differentiated by the presence of a vigilant civil society and judiciary systems, which both limit the so-called 'power of the law' and protect individual liberties.

With the information revolution – the capillary dissemination of information and communication technologies (ICTs) (Floridi, 2007) – contemporary societies are experiencing a new version of the struggle, one that now concerns liberties and authorities in the cyber-sphere, and, more specifically, refers to the deployment of cyber-security measures and individual liberties. Over the past two decades governance, and in particular security, of the cyber-sphere has progressively become a duty falling within the remit of public authorities. It is exactly the involvement of public authorities in the management of the cyber-sphere that both brings to the fore and exacerbates the struggle.[a] The tension that exists between individual rights and public authorities is, in fact, aggravated because of the informational nature of the cyber-sphere.

Data, the bits which comprise the cyber-sphere, are by nature *malleable* (Moor, 1997). They are portable and can be processed, stored, accessed, mined by third parties, and can reveal sensitive personal information, hence facilitating surveillance and controlling measures. It then becomes feasible to wonder whether personal data and information could be completely accessible to those who enforce such measures and have adequate technologies, thus undermining individuals' rights, such as privacy and anonymity. At the same time, since the cyber-sphere has proved to be a structural part of contemporary societies, there is a pressing need to defend and secure it from the potential threats posed by cyber-attacks as well as by cyber-warfare. It is such a need that often

times is recalled as justification for pervasive surveillance practices and the consequent breach of informational rights (2 references removed for peer-review) (Floridi & Taddeo, 2014).[b]

The 2013 National Security Agency (NSA) scandal offers a tangible example of how technological and state power can put such rights under sharp devaluating pressure. The scandal also unveiled the pressing need to address the friction between cyber-security and individual rights in the cyber-sphere, and the necessity to find a balance between the two: in Obama's words, "we have to strike the *right balance* between protecting our security and preserving our freedoms … But given the history of abuse by governments, it's right to ask questions about surveillance – particularly as technology is reshaping every aspect of our lives" (emphasis added).[c]

Cyber-security and individual rights appear to be antithetical, for it seems that the greater our enjoyment of the former, the less we experience of the latter. Ethicists, political philosophers and political scientists have long debated how to strike an ethically sound balance between security measures and individual rights (see for example Floridi, 2014a). This paper contributes to such a debate and offers two main contributions: it specifies a set of rights that individuals living in the information age should claim for themselves, and it proposes a criterion for striking an ethical balance between these rights and cyber-security measures. The contribution rests on the endorsement of a new approach, which focuses on the understanding of individuals' well-being in the information age as a preliminary step in addressing the trade-off between individual liberties and cyber-security measures.

The path leading to the identification of the set of rights and the ethical criterion is not straight and will require two digressions. I shall now provide an outline of the analysis developed in the rest of this paper. First, I will introduce *the online persona* and focus on the analysis of the conditions for individual well-being in the information age. The *capability approach* (Sen, 1980), our first detour, will offer the conceptual framework for such an

analysis, which will in turn provide the basis for identifying the rights that individuals living in the information age should claim for themselves.

The "struggle between liberties and authorities" will then be reconsidered on the basis of the analysis of well-being of the online persona and of the suggested set of individual rights. I shall argue that the struggle is only apparent and that cyber-security measures are the response of public authorities to the individual *claim-right* to security. This argument will require a second and final digression in order to consider the so-called *Hohfeldian incidents* (Hohfeld, 2000), which will offer an analytic description of the nature of rights. On the basis of this analysis, I will propose an ethical criterion to balance cyber-security and individual rights in the information age.

2. The online persona

In considering individual rights in the information age, the relevant literature focuses mainly on the defence of privacy and anonymity (Nissenbaum, 1998) (Walters, 2001). However, the rise of the information revolution and of the cyber-sphere as a new domain in which individuals live their lives (references removed for blind review purposes) unveils a more complex scenario. Individuals living in information societies spend considerable amounts of their lives in the cyber-sphere, either for work or for other reasons. Online interactions and life in the physical world are increasingly interwoven and experiences in one domain increasingly prove to have great impact on the other (Floridi, 2014b).

The blurring of the boundary between the cyber-sphere and the physical environment has been noted and analysed by social scientists (Price, 2002) and psychologists (Hasebrink, 2008), as well as by philosophers, who have analysed its ethical implications, the changes that it has prompted on the ontology of the contemporary world, the nature of the agents existing and interacting in it, and on its political dynamics (Coole et al., 2010), (reference removed for review purposes), (Floridi, 2013).

Recent psychology studies analyse this relation and draw very interesting conclusions (Hasebrink, 2008) (Suler, 2004) (Australian Psychological Society, 2010), (Sapouna et al., 2011). For example, Sapouna and colleagues (2011) focus on teenage victims of cyber-harassment and highlight a strong link between online experiences and offline behaviours. These studies report that young individuals who have been harassed in the cyber-sphere are more likely to commit truancy, leave home, start using drugs and alcohol or, in the most dramatic cases, commit suicide.

These cases support those philosophical analyses that argue that experiences occurring in the cyber-sphere contribute to individual well-being and to the process of shaping personal identity in ways that are similar to the ways in which experiences in the physical world do (Oosterlaken, 2012), (Ess, 2012).

Several philosophical studies of this phenomenon stress the relation between online practices and individual identities and speculate on the way in which the former contributes to the definition of the latter and on the relation between online and offline identities (Ess, 2012). However, this paper does not rest on any specific interpretation of the nature of such a relation. Rather, it focuses on the common ground to all such analyses and maintains that there is a link between online experiences and life conducted in the physical world, and that the former contributes to individuals' overall well-being. In this respect it is worth recalling the Online Manifesto[d] that the Digital Agenda for Europe released in 2013,[e] which promotes the concept of the 'onlife' to stress the blurring of the distinction between online and offline, and which notes the potential for experiences performed in one or other domain to impact individuals' lives and well-being.

In the rest of this paper I shall refer to the *online persona* as a model of an individual interacting in the cyber-sphere. The online persona should not be mistaken for the online alter ego, the avatar or the character one may interpret while being online, nor is it a person's profile on a social network; it is a model of an individual interacting in the cyber-

sphere define using an *informational* level of abstraction (LoA) (Floridi, 2008). Let me clarify.

A LoA is a finite but non-empty set of observables accompanied by a statement of what feature of the system under consideration such a LoA stands for. A collection of LoAs constitutes an interface. An interface is used when analysing a system from various points of view, that is, at varying LoAs. Any given system, e.g. a car, the human body, a glass of wine, can be observed by focusing on certain aspects and disregarding others, and the choice of these aspects, i.e. the observables, depends on the observer's purpose or goal. For example, an engineer interested in maximising the aerodynamics of a car would likely focus upon the shape of its parts, their weight and the materials. A customer interested in the aesthetics of the car will focus on its colour and on the overall look. The engineer and the customer observe the same system, i.e. the car, but endorse different LoAs. It is important to stress that a single LoA does not reduce a car to merely the aerodynamics of its parts or to its overall look. Rather, a LoA is a tool that helps to make explicit the observation perspective and constrain it to only those elements that are relevant in a particular observation.

In considering the online persona, I am endorsing a specific, i.e. informational, LoA. It is worth remarking that I am not reducing the individual, i.e. the human being, to her online persona, for a human being can be considered by focusing on different LoA. Nor am I reducing individuals acting in the cyber-sphere to the information they communicate, store or produce. Also, individuals acting in the cyber-sphere can be described using different LoAs that focus on different observables, e.g. economic and psychological. I am restricting the analysis to an informational LoA because it focuses on fundamental, constitutive aspects of the experiences one may have while being online, i.e. the production, access and communication of information.

Now that the LoAs have been introduced, let me clarify in which sense one may talk of the well-being of the online persona, as this will enable us to escape a possible

objection the reader may have at this point. In fact, one could object that the online persona is an abstract model and, as such, one can only speak of its well-being in metaphoric terms. This raises an interesting point, but it also rests on a mistaken understanding of the model. The objection surmises that a model is a concept with no links outside the abstraction in which it has been defined, much in the same way a purely fictional character has no referent outside the novel in which it is portrayed. However, a model is a simplified representation of a given system, and at such it is not decoupled from the latter (Chestnut, 1967), (Pidd, 2004). Quite the contrary; a model remains correct until it represents the system, predicts its behaviour and allows for manipulating the system to achieve a given goal. This is evident when one considers any kind of model, from blueprints to mathematical equations and any kind of modelled system, conceptual or physical. The reader may recall that the online persona is not a concept, or an abstract entity, but a model of an individual interacting in the cyber-sphere, which in turn is our system.

Thus talking of the well-being of the online persona is a way of considering the well-being that an individual may enjoy while being online. The online persona serves as a model in order to isolate important aspects of the system – recall the informational LoA, on which further analysis can be developed. One talks of the well-being of the online persona in the same way one talks of the properties of a Turing machine to understand the properties of a computing machine, not in the same way in which one may talk of the well-being of Sherlock Holmes.

With this clarification in mind, I can now focus on the analysis of the well-being of the online persona, so as to understand what is necessary for the online persona to flourish. In order to do so I shall momentarily divert from the main path and consider in more detail what the well-being of individual may be in the information age.

3. The capability approach and well-being of the online persona

Several theories of individual well-being have been provided in the literature (Griffin, 1988) (Haybron, 2010) (Sumner, 1996). The analysis of the online persona's well-being proposed in this paper will rest on the *capability approach* (Sen, 1980). The reason for such a choice will be provided presently. First, let me briefly describe the most relevant features of such a theory. The capability approach provides a framework for both a normative and a descriptive analysis of individual well-being and identifies the two fundamental aspects of well-being as *functionings* and *capabilities*. Functionings are individuals' *beings* and *doings*, i.e. states and actions. They are valuable when an individual shows a proactive attitude towards them, for s/he desires, wants and acts so as to achieve them. Valuable functionings are, for example, part of an individual's projects and whose achievement has a positive impact on her life. According to the capability approach, individual well-being is "*the capability to achieve valuable functionings*" (Olsaretti, 2005).

What such functionings may be in more specific terms is open to discussion. However, there are some functionings that are deemed to be constitutive of human nature (Nussbaum, 2003) and which are fundamental for the achievement of well-being, e.g. being nourished, having shelter, drinking non-polluted water. Nonetheless, functionings may vary from case to case, depending on individuals' personal projects. It can be said that a valuable functioning is one that an individual chooses and endorses in her life.

Functionings are, however, only half of the constituents of an individual well-being. More precisely, they are the descriptive side of the definition proposed by the capability approach since they focus on the subjective part, on individual preferences and inclinations, and allow for specific variables of people's different lives. The capabilities of achieving functionings are the other half of the definition; more specifically, an individual's capability of achieving the functionings that she values is the *measure* of her well-being.

The nature of these capabilities has been widely debated (Olsaretti, 2005) (Kaufman, 2006). Capabilities refer to the *effective freedom* of an individual to achieve

valuable functionings. Such a freedom has a tripartite nature consisting of (i) not being prevented from achieving a given functioning, (ii) having the means to pursue the chosen functioning, and (iii) having the possibility to forgo some functionings. More precisely, as stressed by Olsaretti, the defender of the capability approach advances three claims. The first one concerns *disvaluable functionings*, namely, functionings that have no moral value or directly conflict with other individuals' well-being. According to the capability approach, societies and public authorities have no moral duty to support individuals striving to achieve such functionings. The second claim refers to the possibility for a third-party to remove choice-insensitive obstacles, which may impair the achievement of valuable functionings so as to increase individual effective freedom. This refers in particular to scenarios in which public authorities may act to improve conditions – environmental, cultural and societal – to facilitate individual well-being. An example could be eradicating malaria from an area as a way of removing the risk of infection, which would be an obstacle to the achievement of individuals' well-being. Finally, valuable functionings cannot be imposed and individuals have the liberty to 'choice-sensitive' departure from functionings.

The capability approach is particularly suitable for the purpose of the analysis presented in this paper, because it does not focus on specific goods on which well-being may depend. Rather, it identifies the conceptual framework for the definition of well-being and leaves open the question concerning the actual content of a good life. The relation between functionings, capabilities and rights is particularly relevant for the purpose of our analysis, in that the approach stresses that the capability of achieving the functionings that one values is the measure of well-being. Individual rights play a crucial rule in this scenario, for they are meant to safeguard and foster such capabilities.

The time has come to consider what the valuable functionings of the online persona are. In doing so, I will not focus on those functionings whose value strictly depends on individuals' inclinations, projects and experiences. The focus will instead be

on those (fundamental) functionings which concern constitutive aspects of the online experience, for they concern those states and actions that allow the very existence of the online persona, in much the same way that the fundamental functionings identified by Nussbaum (2003) support individuals' well-being by focusing on states and actions that are fundamental to the existence of human beings.

In this respect, at least three functionings are fundamental, as they concern constitutive beings and doings of the online persona. These are:

i. *Accessing, communicating and sharing valuable information.* Accessing and communicating information is at the very core of any online action that one may perform. As the online persona exists insofar as one acts in the cyber-sphere, being able to access and exchange information is crucial to its very existence.

ii. *Shaping, expressing and sharing its own narrative.* This functioning refers to the autonomy of the online persona, which can then independently steer its actions in the cyber-sphere and therefore shape its narrative.[f]

iii. *Enjoying a high level of connectivity*. This is a twofold functioning, as it refers both to the very status of being *online*, i.e. the exploitation of ICTs, and to the possibility of each online persona being part of a network and being granted access to interactions with other personas and agents.

Following the framework proposed by the capability approach, the well-being of the online persona depends on the capability to achieve such functionings. Rights in the information age will foster individual well-being insofar as they protect and foster these capabilities.

4. Individual rights in the information age

On the basis of the analysis provided so far, four rights are deemed to be fundamental for the well-being of the online persona. Like the list of fundamental functionings, this list is not meant to be exhaustive and to specify all possible rights that may foster individual

well-being in the information age. The aim is much more constrained, and focuses on identifying the most fundamental rights that are necessary for this end. Such rights are:

i. The right to have access to the digital sphere, to computational and informational resources;
ii. To engage in pluralistic, transparent, and fair online interactions;
iii. To exert some level of control on the way their online persona is treated, as their personal information available online is a constituent of their own narrative;
iv. To act in a *secure* cyber-sphere.

The first right refers to the access to computational, storage and networking resources that are necessary for sharing, recalling and storing personal data and information. Networking resources are necessary as well, as they permit the interactions in the cyber-sphere. The second right refers to the liberty that the online persona should enjoy in order to engage in interactions in the cyber-sphere that are free of undue censorship and encroachment. The third right protects individual privacy. Such a right rests on the consideration that privacy is related to the process of construction of one's own identity (Agre, 1997) and, for the online persona, it concerns the shaping of its own narrative. It attributes some control to the individual over the narrative as a way of limiting unreasonable constraints, which may be imposed by third parties on such a process.

Let me remark that rights (i)–(iii) should by no means be understood as a preliminary step to argue for the right to access the cyber-sphere as a human right. The proposal here is much more subtle and less idealistic. As Vint Cerf put it: "Although it strikes me as somewhat extreme to argue that access to and use of the Internet should be codified as a 'human right' in the sense of the United Nations Universal Declaration of Human Rights, it does seem to me that among the freedoms that are codified, including the right to speak freely, should be the right to expect freedom (or at least protection) from harm in the virtual world of the Internet" (Cerf, 2011, p. 465).

Finally, the last right stresses the right of the online persona to exist in an environment reasonably free from threats and dangers. This is the right to security, a complex right whose definition is not uncontroversial. A more in-depth analysis is then necessary to consider its nature in greater detail, and to do so we must now embark on the second and final digression of our analysis.

4.1 Liberty- and claim-rights

One aspect to take into account when considering the right to security is that it does not fall squarely within the canonical distinction between negative and positive rights (Shue, 1996). Such a distinction rests on the nature of duty imposed on public authorities; at first glance the right to security seems to be a negative right, as it defends the individual's personal space from invasion by state or other third parties. However, a more detailed analysis shows that the right to security prompts the duty of public authorities to exert their power in order to protect individuals from the actions of other individuals, be they fellow citizens or enemy forces. Such a duty poses the need for positive measures raging from criminal justice and the protection of property to the enforcement of cyber-security procedures, which may all require the invasion of individuals' personal space.

The complex nature of the right to security makes it a difficult concept to grasp in relation with the other rights specified in the list. It also creates a conceptual muddle around the struggle between liberties and authorities. For it now seems that security measures and individual rights are not as antithetical as they first appear. Hohfeld's analysis of the nature of rights will be crucial to overcome this confusion (Hohfeld, 2000).

Hohfeld argues that rights have a complex internal structure, which derives from the way some basic elements are arranged. Such elements are called *incidents* and qualify the nature of the right. The incidents allow for distinguishing four components of a right: the *liberty*, the *claim*, the *power* and the *immunity*. Liberty and claim are primary rules, whereas power and immunity are secondary rules – they are second-order elements and refer to the way in which primary rules can be introduced and changed. A detailed

discussion of secondary rules falls outside the scope of this paper; for the purpose of the present analysis it will suffice to focus on liberty and claim.

Each Hohfeldian incident is identified by a specific logical form; a liberty-right has the following logical form:

> A has the liberty to *p*, if and only if A has no duty not to do *p*; Alice has the liberty to walk barefoot in her own garden if and only if Alice has no duty not to walk barefoot in her own garden.

Liberty-rights are characterized by the absence of the duty not to perform a given action for the right-holder, while a claim-right is a right that exists specifically because the duty exists for someone other than the right-bearer to perform a given action. Recalling Alice again, she has the claim that Bob (her piano teacher) explains to her how to play the piano if and only if Bob has the duty to teach Alice how to play the piano. The logical form of claim-rights is A has the claim that B performs *r* if and only if B has the duty to A to perform *r*. The important aspect of claim-rights is the relation between the right-holder claim and the duty of the other party.

The distinction between claim- and liberty-rights allows for a reconsideration of the list of rights provided in section four. The first three rights on the list are liberty-rights and define precisely the boundaries of the authorities' powers over individuals' freedom, as individuals have no duty not to perform the actions specified by those rights, whereas the right to act in a secure environment is a claim-right. The right expresses a claim that individuals have towards public authorities to be in a secure cyber-sphere, and public authorities have, in turn, the duty to guarantee the security of the cyber-sphere. This sheds new light on the struggle between liberties and authorities, as it reveals that cyber-security measures and individual rights are not jarring and that the former are the response to individuals' claim-rights to act in a secure environment.

We can now devote our attention to the analysis of the balance between individual rights and cyber-security measures.

5. Ethical balance between individual rights and cyber-security

Although cyber-security measures and individual rights are not in open conflict, as it seems at first glance, there is nonetheless some friction between the two. Contemporary societies face the compelling need to define a harmonious combination of the two in order to ensure the well-being of individuals and the development of democratic information societies at the same time. Defining a criterion to strike a fair balance between the two will allow this need to be addressed. The criterion should be defined keeping in mind the fact that cyber-security measures are a response of public authorities to individuals' claim-rights to being in a safe cyber-sphere and that the security of the cyber-sphere is a crucial aspect for their well-being.

Yet, the security of the cyber-sphere is important insofar as it is a *pre-condition* to an individual's well-being and, in the long-term, to the fulfilment of the online persona. Cyber-security measures are therefore instrumental; they are the means through which such a precondition is satisfied. The instrumental value of cyber-security procedures allows us to define the criterion for reaching the balance. Cyber-security measures are in an ethically sound balance with individual liberties when the former are *preparatory* to the latter and are implemented only to *remove obstacles* that may prevent individuals from achieving their well-being.

Cyber-security measures contribute to individual well-being insofar as they are the means through which public authorities respond to individual claim-rights to be in a safe environment and *remove* critical and pervasive threats in a way that is consistent with the fulfilment of the online persona. Public authorities, then, have the duty to develop structures and institutions that will enable them to respond to and minimize such threats. In doing so, public authorities could breach individual rights only when clear and present threats menace the very existence of the online persona or of individuals. The breach in such a case ought to be minimal and momentary in all circumstances.

It is noteworthy that the proposed criterion is consistent with liberal views underpinning democratic information societies and is also consistent with the interpretation of freedom proposed by the capability approach. As specified in section three, capabilities are understood to be substantive freedom and, as such, they also encompass freedom from choice-insensitive obstacles, which may deter an individual from achieving her valuable functionings. The capability approach allows, indeed some authors would also argue that it prescribes (Olsaretti, 2005) (Nussbaum, 2003), public authorities to act to remove such obstacles as part of their normative actions. Threats and harms occurring in the cyber-sphere are obstacles that can obstruct the well-being of the online persona and thus the well-being of an individual. Therefore, it is a duty of public authorities to remove them as a way of promoting individuals' well-being.

Considering cyber-security measures as a precondition for individual well-being and including the enforcement of such measures among the normative actions of public authorities may be misinterpreted as a way of assigning a primary role to such measures and, perhaps, a prevalent part in the balance between security and rights. A clarification is thus necessary, lest the proposed analysis incurs such an objection.

More specifically, the analysis presented in this paper may be mistaken as supporting the so-called *securitization of rights* (Goold, 2007, pp. 325–346). This is a way of understanding the right to security which has become popular over the past decades and which is affecting the way security issues are addressed in our societies and, to some extent, in the cyber-sphere. According to such an approach, the right to security provides the ground for other fundamental rights. Consider for example Article 143 of the United Nations 2005 World Summit Outcome, which defines the right to security as "*the right of people to live in freedom and dignity, free from poverty and despair. We recognize that all individuals, in particular vulnerable people, are entitled to freedom from fear and freedom from want, with an equal opportunity to enjoy all their rights and fully develop their human potential. To this end, we commit ourselves to discussing and defining the notion of human security in the General Assembly*".

According to this view the right to security is a meta-right (Goold, 2007, p. 327) which provides the foundation for individual rights. This way of considering the right to security offers some justification for encroaching and breaching individual liberties, as these are considered dependent upon the rights to security and not as self-standing rights; here the right to security is understood as a catch-all right, a right that allows all the other rights to exist. Such an approach compromises attempts to find a balance between security and liberties, as it is makes the right to security a primary, more fundamental right. It then follows that there is no need to strike a balance between security and liberties as the latter depends on the former.

The criterion proposed in this paper rests on an understanding of the right to security as an *instrumental* right to the enjoyment of more fundamental liberties. In this respect, cyber-security measures are a precondition to the achievement of individuals' well-being and enjoyment of other rights only insofar as they allow for removing possible obstacles to such an enjoyment. The right to security is a *pragmatic* precondition but not a conceptual foundation for such rights. The conceptual foundation of the liberty-rights of the online persona has been specified in section three, where it has been argued that those rights are meant to protect individual capabilities to achieve valuable functionings and, hence, their well-being. As such, the right to security should not be considered the meta-right from which liberty-rights stem. Rather, it should be understood as a right devoted to paving the way, or facilitating, the enjoyment of liberty-rights. In this respect, it is worth considering that an individual could enjoy the rights described in section three in the cyber-sphere even when security in not ensured. A dangerous cyber-sphere does not preclude, in principle, the possibility of enjoying such rights. Nonetheless, the enjoyment of liberty rights would be facilitated and could perhaps also achieve higher levels in a safe cyber-sphere.

One more clarification is necessary before concluding this paper; it concerns informational rights and their relation to security measures. The analysis proposed here

offers us the ground to stress that informational rights defend aspects of individuals' existence which contribute to their overall well-being. As such, the breaching of these rights should be deemed as severe an act as the breaching of bodily privacy, for example. Protection of personal information as well as freedom of speech and access to the internet ought not to be considered weaker, secondary rights that can be encroached to an undefined extent and without a clear justification any time that guarantee of physical security is allegedly at risk, as it has been the case unveiled by the PRISM scandal. An impairment of any of the rights specified in section four will have an impact on individuals' well-being and as such it should always be carefully motivated and implemented using the criterion highlighted in this section, to ensure that the breaching will be as minimal as possible. Let me now wrap up the analysis that has been developed so far.

6. Conclusion

I have argued that the tension between cyber-security measures and individual liberties is not unlike the struggle between authorities and liberties that Mill stressed in his analysis, and is close to the view put forward by contractualist theories, according to which a state's authority rests on the trade-off of liberty for security, Hobbes and Locke offering two famous examples of such theories.

This paper provides an ethical criterion specifying how cyber-security measures ought to be put in place to respect individual rights. Specifically, cyber-security measures ought to be considered as preparatory, *instrumental*, for the achievement of individual well-being; as such they ought to be implemented to facilitate the achievement of individuals' liberty-rights and the fulfilment of the online persona. Such a criterion rests on an analysis of individual rights and well-being in the information age, which has unveiled the relevance of online experiences for an individual's overall well-being and highlighted the need to consider other rights, not just privacy and anonymity, as fundamental rights for

individuals living in the information age. It should be noted that while the proposed analysis stresses the relevance of the right to security for the achievement of individuals' well-being, such a right is not deemed to be the conceptual ground on which the liberty-right rests. Quite the opposite: security-right is considered to be instrumental for fostering individual liberty-rights, the latter being self-standing rights tightly related to individual well-being.

The analysis proposed in this paper highlights the need to reconsider the approach to the debate on cyber-security measures and their ethical implications. The growing importance of the cyber-sphere as part of the reality in which we live demands that the experiences and the time we spend there are considered to be as important in the fulfilment of our lives as any other kind of experience. As such, we as individuals living in the information age should claim the duty of public authorities to make the cyber-sphere secure in the same way that we advance this claim for our streets. At the same time, we should defend our privacy and anonymity as well as our rights to access the cyber-sphere and to foster and improve our lives in it, just as we would defend our rights to education, to participate in our cultural heritage, and to self-determination in offline life.

Acknowledgement

An early version of this manuscript has been presented and discussed at the research seminar of the Uehiro Centre for Practical Ethics, University of Oxford and at the 2013 meeting of the Society for Philosophy and Technology (SPT) in Lisbon. I would like to thank the colleagues who attended both meetings for their comments and feedback. I benefited enormously from many insightful comments by Philip Serracino Inglott (Delft University) and Matteo Turilli (Rutgers) for their helpful suggestions and conversations on the key points of this paper. Finally, I would like to express my sincere gratitude to the reviewers for their comments to the earlier version of this paper. I remain the only person responsible for any of its shortcomings.

References

Abbate, J. (2000). *Inventing the Internet*. Cambridge, Mass: MIT Press.

Agre, P. (1997). *Technology and privacy the new landscape*. Retrieved May 19, 2013, from http://site.ebrary.com/id/10015368

Arquilla, J. (1998). Can information warfare ever be just? *Ethics and Information Technology*, *1*(3), 203–212.

Australian Psychological Society. (2010). *The Social and Psychological Impact of Online Social Networking, APS National Psychology Week Survey*. Retrieved from http://www.psychology.org.au/publications/inpsych/2010/december/social/

Cerf, V. G. (2011). First, Do No Harm. *Philosophy and Technology*, *24*(4), 463–465.

Chestnut, H. (1967). *Systems Engineering Methods*. New York: Wiley, John Sons.

Coole, D., Frost, S., Bennett, J., Cheah, P., Orlie, M. A., and Grosz, E. (2010). *New Materialisms: Ontology, Agency, and Politics*. Durham, NC: Duke University Press.

Copeland, B. J. (2006). *Colossus: The secrets of Bletchley Park's code-breaking computers*. Oxford University Press.

Denning, D. E. (1999). *Information warfare and security*. Reading: Addison-Wesley.

Dipert, R. (2010). The Ethics of Cyberwarfare. *Journal of Military Ethics*, *9*(4), 384–410.

Ess, C. (2012). At the Intersections Between Internet Studies and Philosophy: "Who Am I Online?" *Philosophy & Technology*, *25*(3), 275–284.

Floridi, L. (2007). A Look into the Future Impact of ICT on Our Lives. *The Information Society*, *23*(1), 59–64. doi:10.1080/01972240601059094

Floridi, L. (2008). The Method of Levels of Abstraction. *Minds and Machines*, *18*(3), 303–329. doi:10.1007/s11023-008-9113-7

Floridi, L. (2013). *Ethics of information*. Oxford University Press.

Floridi, L. (2014a). *Protection of Information and the Right to Privacy - A New Equilibrium?* Dordrecht: Springer. Retrieved from http://www.springer.com/law/international/book/978-3-319-05719-4

Floridi, L. (2014b). *The Fourth Revolution, How the infosphere is reshaping human reality*. Oxford University Press.

Floridi, L. (2014c). *The Onlife Manifesto - Being Human in a Hyperconnected Era*. Dordrecht: Springer. Retrieved from http://www.springer.com/philosophy/epistemology+and+philosophy+of+science/book/978-3-319-04092-9

Floridi, L., and Taddeo, M. (eds.) (2014). *The ethics of information warfare*. New York: Springer.

Freed, L., and Ishida, S. (1995). *History of Computers*. Hightstown, NJ: Ziff-Davis.

Goold, B. J. (2007). *Security and human rights*. Oxford: Hart.

Griffin, J. (1988). *Well-being: its meaning, measurement and moral importance*. Oxford: Clarendon Press.

Hasebrink, U. (2008). *Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online : [European research on cultural, contextual and risk issues in children's safe use of the internet and new media (2006-2009)]*. [London]: EU Kids Online. Retrieved from http://www.eukidsonline.net/

Haybron, D. M. (2010). *The pursuit of unhappiness: the elusive psychology of well-being*. Oxford University Press.

Hohfeld, W. N. (2000). *Fundamental legal conceptions as applied in judicial reasoning*. Union, NJ: Lawbook Exchange.

Kaufman, A. (2006). Capabilities and Freedom. *Journal of Political Philosophy*, *14*(3), 289–300.

Lucas, G. R. (2012). Just War and Cyber Conflict "Can there be an 'Ethical' Cyber War?" Presented at the Naval Academy Class 2014.

Maan, A. K. (1999). *Internarrative identity*. Lanham, MD: University Press of America.

MacIntyre, A. (1989). The Virtues, the Unity of a Human Life and the Concept of a Tradition. In *Why Narrative?* Grand Rapids, MI: W. B. Eerdmans.

MacIntyre, A. C. (2007). *After virtue: a study in moral theory*. Notre Dame, IN: University of Notre Dame Press.

Mill, J. S. (2002). *On liberty*. New York: Dover.

Moor, J. H. (1997). Towards a theory of privacy in the information age. *ACM SIGCAS Computers and Society*, *27*(3), 27–32.

Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, *17*(5-6), 559–596.

Nussbaum, M. (2003). Capabilities as Fundamental Entitlements: Sen and Social Justice. *Feminist Economics*, *9*(2–3), 33–59.

Olsaretti, S. (2005). Endorsement and Freedom in Amartya Sen's Capability Approach. *Economics and Philosophy*, *21*(1), 89–108.

Oosterlaken, I. (2012). *The capability approach, technology and design*. Dordrecht and New York: Springer. Retrieved from http://dx.doi.org/10.1007/978-94-007-3879-9.

Pidd, M. (2004). *Systems Modelling: Theory and Practice*. 1st edn. Chichester and Hoboken, NJ: Wiley.

Price, M. E. (2002). *Media and Sovereignty: The Global Information Revolution and Its Challenge to State Power*. Cambridge, MA: MIT Press.

Sapouna, M., Wolke, D., Vannini, N., Watson, S., Woods, S., Schneider, W., Aylett, R. (2011). Individual and social network predictors of the short-term stability of bullying victimization in the United Kingdom and Germany. *British Journal of Educational Psychology*, *82*(2), 225–240.

Schechtman, M. (2007). *The constitution of selves*. Ithaca, NY: Cornell University Press.

Sen, A. (1980). Equality of What? *The Tanner Lecture on Human Values*, *I*, 197–220.

Shue, H. (1996). *Basic rights: subsistence, affluence, and U.S. foreign policy*. Princeton University Press.

Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology & Behavior*, *7*(3), 321–326. doi:10.1089/1094931041291295

Sumner, L. W. (1996). *Welfare, happiness, and ethics*. Oxford: Clarendon Press.

Taddeo, M. (2011). Information Warfare: A Philosophical Perspective. *Philosophy & Technology*, *25*(1), 105–120. doi:10.1007/s13347-011-0040-9

Taylor, C. (1989). *Sources of the self: the making of the modern identity*. Cambridge, MA: Harvard University Press.

Walters, G. J. (2001). *Human rights in an information age: a philosophical analysis*. University of Toronto Press.

---

[a] The involvement of public authorities in the management and regulation of the cyber-sphere does not come as a novelty when one considers that the design and development of the internet has been since the very beginning a part of governmental research to ensure national and international security; see for example the famous Pentagon Arpanet project (Abbate, 2000). At the same time, it is worth recalling that security requirements and the support of military activities are often the goals motivating the design and development of plenty of technologies that have then become commonly used. Computers offer quite an evident example: they went from being a technology used to support military efforts during the Second World War to being a *tool* people use in their everyday lives (Copeland, 2006), (Freed & Ishida, 1995); the same goes for robotics and AI, Predator (http://en.wikipedia.org/wiki/General_Atomics_MQ-1_Predator) and Taranis offering two interesting examples (http://en.wikipedia.org/wiki/BAE_Systems_Taranis).

[b] The reader interested in the on-going debate on cyber-warfare and on the ethical and regulatory issues that it poses may find relevant the following papers (Arquilla, 1998), (Denning, 1999), (Dipert, 2010), (Lucas, 2012), (reference removed for peer-review).

[c] http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference

[d] http://ec.europa.eu/digital-agenda/futurium/en/content/onlife-manifesto-being-human-hyperconnected-era

[e] A more in details analysis of the work developed under the 'Onlife Initiative' has been provided here (Floridi, 2014c)

[f] The concept of narrative has been extensively used in the literature focusing on personal identity (Maan, 1999) (MacIntyre, 2007) (MacIntyre, 1989) (Schechtman, 2007) (Taylor, 1989). However, it is worth remarking that the analysis proposed in this paper does not rest on the narrative approach insofar as it is not concerned with the process of constructing personal identities. The reader interested in such a topic may find useful (Ess, 2012).