Information **2011**, *2*, 594-620; doi:10.3390/info2040594

OPEN ACCESS

information

ISSN 2078-2489

www.mdpi.com/journal/information

Article

The Online Construction of Personal Identity through Trust and Privacy

Massimo Durante

University of Torino, Law School, via s. Ottavio 20, Torino 10124, Italy;
E-Mail: massimo.durante@unito.it; Tel.: 0039-11-6703210; Fax: 0039-11-6702559

Received: 4 August 2011; in revised form: 6 September 2011 / Accepted: 26 September 2011 / Published: 11 October 2011

Abstract: Constructing a personal identity is an activity much more complex than elaborating a series of online profiles, which are only digital hints of the Self. The construction of our personal identity is a context-mediated activity. Our hypothesis is that young people are enabled, as digital natives and social network users, to co-construct the "context of communication" in which their narrative identities will be interpreted and understood. In particular, the aim of this paper is to show that such "context of communication", which can be seen as the hermeneutical counterpart of the "networked publics" elaborated by Danah Boyd, emerges out of the tension between trust and privacy. In other terms, it is, on the one hand, the outcome of a web of trustful relations and, on the other, the framework in which the informational norms regulating teens' expectations of privacy protection are set and evaluated. However, these expectations can be frustrated, since the information produced in such contexts can be disembedded and re-contextualized across time. The general and widespread use of information technology is, in fact, challenging our traditional way of thinking about the world and our identities in terms of stable and durable structures; they are reconstituted, instead, into novel forms.

Keywords: trust; privacy; personal identity; social networks; informational norms; contextual integrity; accountability; offline/online realities

1. Introduction

Many scholars envisage a progressive, inevitable convergence of the offline and the online realities or, as others put it, of the physical and the virtual realms. The debate on this issue often fails to

recognize that, from a philosophical point of view, the difference between the real and the virtual dimension of reality precedes–and does not entirely depend on–the distinction between offline and online reality. This means that the differentiation between reality and virtuality is already insular to the offline reality. However, this distinction also concerns the online reality. From this perspective, the convergence between offline and online reality is more a revised interpretation of the role of computers (which are no longer viewed as interfaces but as tools cooperating to reontologize our reality in informational terms [1]) rather than the description of the actual possibility to overcome the differentiation between reality and virtuality that belongs both to the offline online realities.

This differentiation is important for the construction of personal identity. We can speak of construction because our personal identity necessarily exists across time and is constituted, at the same time, of what we are (*i.e.*, the "actual self" made of information describing our features) and of what we would like to be or what we ought to be (*i.e.*, the "ideal self" made of information describing our expectations or the social expectations about us). In other words, personal identity is always constituted of both reality and imagination (virtuality). It is central to understand in this respect that the "ideal self" is not a regulative idea, in a Kantian sense, to which the actual self tends to conform itself. On the contrary, it is *already* a constitutive part of the self. Our personal identity is an "open text", the lines of which are made out of the intertwinement of reality and ideality. Those who affirm and those who refuse to acknowledge that social networks (or the Internet) are online spaces where people are given the possibility to endorse a second life or a new personality are both wrong, because they do not realize that social networks (or the Internet) constitute only *a different way* to intertwine reality and imagination in the construction of personal identity. Placed against the backdrop of the intertwinement of reality and ideality, the Self experiences itself as a dynamic reality that has to be constructed within the different and particular networked *contexts of communication* that form such backdrop.

We should state from the very beginning how social networks enable people to construct (at least in part) their personal identity in a way that is different from what happens in the physical reality. In the physical reality, we construct our identity (narratively understood as an open text) within different environmental and social constraints, *i.e.*, within different contexts, that are mainly already structured and given and cannot really be fashioned by our narratives. In contrast, in the digital reality, social networks for instance are platforms (as in the case of Facebook) that enable users to take advantages of networked affordances in order to construct, in informational terms, not only their identities but also to participate in the co-constructions of their networked contexts of communication.

We should not forget, in this respect, that the construction of identity does not stem from the scratch but occurs in a situated context: identity is always part of a *context*. This is essential in order to understand the text that is formed within it. However (and this point is crucial), the context cannot be reduced to an empirical situation, to a particular networked architecture or technological platform. In the digital space, the context is, according to Dey [2], a sum of information that characterizes a specific situation (on the basis of the technological affordances of a particular architecture or platform). Hence, the following statement stems from our main point: both personal identity and the context of communication can be conceived and understood, at different levels of abstraction [3,4], in informational terms.

However, our informational presence in the net is in no sense only a "virtual" presence. On the contrary, it does produce consequences in real life. As autonomous agents in fact, we are called upon to account for the *consequences* of our actions. The intersubjective regime of accountability (which entails moral responsibility or legal imputation) is a measure of the way in which our presence in the net is "kept in touch" with reality, to the extent to which we are called upon to justify, in real life, what we have done in the net. This makes it necessary to translate the virtual dimension of our online existence into the empirical terms of our offline existence [5]. In this sense, accountability is not only a key part of our personal autonomy but, when referred to the online world; it can also serve as a *principle of reality*.

This regime of accountability can be set either by means of moral or legal norms, which are established across time by tradition or which are laid down by social or political institutions. Accountability can also be developed spontaneously through trustful relations. Trust can be actually viewed as a way to make someone accountable to someone else for what the trustee has been entrusted for by the trustor. In this respect, online trust cooperates to set a systemic context of communication between trustful agents and, therefore, it is meant to mold our networked reality, that is, the reality within which we can construct and project our own online personal identities. For this reason, people need to trust other people in the networked world, not only to delegate them tasks and to achieve specific goals but, first and foremost, in order to share with them the construction of a *meaningful context* where they are be able to disclose and recognize themselves. Disclosing information in the net is thus likely to have consequences in real life. In particular, disclosing personal data can make people infringe privacy rights, and this violation can in turn impair the construction of personal identity.

Hence, there can be, in the online construction of personal identity, a tension between trust and privacy, which seems to belong to the notions of trust and privacy themselves (such as online reputation [6]). At the same time, there is a connection between trust and privacy in their competing tendency to structure the conditions and limits of the online identity construction. The issue is thus to understand the theoretical and practical tension between trust and privacy in the light of that online identity construction. This construction is not based on self-transparency (as for the Cartesian subject) nor does it make us transparent to others, since it requires us to shape the conditions and limits in which we are "revealed" to others. In this respect, a philosophical notation is to be made: as suggested by the Latin origins of the word, to reveal ("re-velare"), means both to unfold (*i.e.*, to remove the veils) and to hide something (*i.e.*, to multiply the veils). This signifies that the identity construction is not simply determined by the disclosure of information (that bears on trust) but is revealed by a multifaceted selection of information (a combination of disclosure and closure) that bears on trust and privacy.

In other terms, the construction of personal identity is always the result of a competition (both internal with ourselves and external with others) between what is disclosed and what is hidden about us: we do not have to forget that a society cannot exist without some spheres of secrets. From this standpoint, personal identity is to be understood as the unending result of a selection of information that forges a *meaningful difference* (*i.e.*, the Self) between what we wish to unfold and what we wish to keep secret. In this respect, we should reaffirm that the possibility to keep a secret from a group of people is not only a part of that construction but, primarily, a basic condition of liberalism [7]. At the same time, we have to recognize that, in the networked Information Society, it is unrealistic to prevent

people from being a deliberate or unintentional source of information, whereas people should not be deprived of the power to rectify the false/incorrect information concerning them or to have this information cancelled.

2. Trust

I will start my analysis by focusing my attention on trust, in order to highlight some of its aspects that concern in particular the structure of intersubjectivity and the disclosure of information that a relation of trust may entail.

Trust is one of the basic social concepts "that helps human agents to cope with their social environment and is present in all human interactions" [8]. Without trust in agents, infrastructures and organizations, human interactions are undermined and, ultimately, almost no social cooperation or relation would be possible. Trust is a context-dependent concept in that trust is essential when dealing with situations that display a certain lack of certainties such as: social environment (we rely upon incomplete information and subjective beliefs); someone else's behavior (we never fully rely upon predictable actions in order to achieve a goal); organizations or infrastructures (we rely upon organizations or infrastructures where their functioning or settings are not completely visible, known or manageable). Social networks, for instance, require all three of the above forms of reliance upon lack of certainties.

If a context is made of information that characterizes a specific situation, the context of trust is made of incomplete information, namely, of lack of certainties, which necessarily exposes the trustor to some risk. In this sense, trust is meant to exist insofar as there is a risk [9] or something that escapes from our cognitive faculty to have control over. On the one hand, the level of trust we are willing to display depends on the perceived embeddedness in the specific situation where the relation of trust takes place. On the other hand, it depends on the perceived lack of certainties that is peculiar to such a situation, which is always relative: the context of trust is not a context of total ignorance. In fact, to trust implies to have some information (except for the case of blind trust) and to share this information in the circle of those who partake in the relation of trust. Placed against the backdrop of complex social systems, trust is a way to reduce uncertainty [9] or, in other terms, to transform an individual risk into a collective one [10].

Furthermore, the relation between trust and the context where the relation of trust takes place is more complex than it may appear *prima facie*. Not only does trust depend on the context in which it is embedded but it tends reflexively to reshape that context by creating a trust atmosphere or a web of trust relations filled with new information. For that reason, and this is a crucial point, the context of trust is not only one formed by incomplete information but, primarily, it is a context of communication where an environment is created in which meaningful relations can take place or, in hermeneutical terms, in which it is possible to share an "horizon of meaning" [11]. This is a cognitive dimension in which our lives can be mutually interpreted and understood. This idea is consistent with the socio-cognitive interpretation of trust displayed by Castelfranchi and Falcone [12-14], which we refer to hereafter.

Trust consists of three elements [14]: (1) a *mental attitude*, a predisposition towards another agent: this attitude is a belief, the strongest cognitive element, constituted by the evaluation of trustworthiness

and a prediction regarding the agent's willingness and ability to produce some effect; (2) a *decision* to rely upon another person: the intention to delegate the production of a desired outcome, which exposes the trustor to a risk and makes him/her vulnerable; (3) a *behavior*: the effective act of entrusting another agent, which entails a practical relation between the parties.

The relation of trust is thus conditioned by the representation of a double context: the context of the trustor and that of the trustee. In order to trust [14], the trustor should have positive expectations both about (a) the trustworthiness of other agents (internal attribution) and about (b) the external conditions that might influence the trustees' actions (external attribution). The internal attribution of trust depends on the evaluation of the trustees' qualities and defects that define trustworthiness and ground the basic beliefs of trust. They are crucial factors since they constitute specific reasons to be trusted like concern for common goals, friendship, altruism, motivation, reciprocity, and cooperation. External attribution of trust depends on the trustor's perception and evaluation of the appropriate environmental conditions that might influence the trustees' actions. External trust is related to two types of systemic conditions: *positive conditions* relating to the presence of opportunities and resources; *negative conditions* relating to the absence of interference and adversity.

The trust attitude (TA) consists of a set of mental beliefs through which the trustee is evaluated. The cognitive evaluation has degrees: as already mentioned, the level of trust is relative to various factors concerning both the trustee's reliability and the context in which the relation of trust is embedded. These factors can be rationally quantified: they represent what is known by experience or perceived in the situation of risk and uncertainty the trustor is exposed to. The trust attitude consists of a scalable evaluation: degrees of trust are related to rational beliefs and this allows the trustor to evaluate the risk and the advisability of trusting. A calculation is made, so that we can say that trust may be attributed in a stronger or weaker manner. However, this should not allow us to lose sight of the fact that the decision to trust is a *clear-cut decision*: when the trustor is faced with the possibility of trusting, he decides either to trust or not to trust. The decision to trust stems from a calculation but it is not a calculation in itself.

In the trust decision (TD), *the otherness of the agent* (*i.e.*, whether or not the agent comes to betrayal) is not reducible to a mere calculation: the trustor has to enter into relation with the otherness of the agent. When entering into relation, the trustor sets a communication with the trustee. This communication is contingent upon the context in which the trust relation takes place. More analytically, communication is conditioned by the perception of a double context: the context of the *speaker* (*i.e.*, the trustor) and the context of the *receiver* (*i.e.*, the trustee). The speaker can perceive those contexts as being either distinct or integrated. When the speaker realizes that the context is integrated (namely, it is the same for both of them), the perceived sameness attunes the dimension of otherness of the receiver, who is understood as part of the same horizon of meaning of the speaker. This *fusion of horizons* [11] is a means of smoothing the progress of their communication, since it enables the parties to establish a trustful relation within a single context of communication.

The perception of a bond, through which agents form a single unit, influences both trust and privacy. The more the context of speakers and receivers is perceived as integrated, the more the ensuing context of communication can be taken as private or at least as semi-public. As a result, the more the context of communication is viewed as private or semi-public, the lower the concern for

privacy and, accordingly, the higher the trust in the communication. Here we can state a crucial point of our analysis: the same social space or technological platform (social networks) can host different contexts of communication. The intensity of the trust relation and its possible trade-off with privacy depends, first and foremost, on the specific *contexts of communication* where the trust relation takes place, and not only on the design or settings of the technological platform in which it is embedded. The technological choice for assuring privacy by design or by means of autonomous selection of privacy settings is, undeniably, crucial but it cannot entirely account for all the possible contexts of communication growing out of the technological platform where a trust relation is embedded.

Furthermore, the decision to trust sets a social (informational) norm between the trustor and the trustee: the trustee's actions (e.g., disclosures of information) will be judged according to the context of communication in which the decision to trust take place. In other terms, it is within a particular context of communication that the trustee's actions are expected and, therefore, evaluated. The peculiarity of trust resides precisely in the fact that the social norm regulating the trust relation does not precede but grows out of the communication process between the trustor and the trustee. The normative dimension of trust (*i.e.*, the parties' expectations) is not previously fixed but grows out of the concrete process and context of communication: "The impossibility of enchaining trust within a legal disposition does not entirely exclude trust from the domain of norms" [9]. So trust displays a normative dimension, which is not forged by legal norms or by technological devices but has a *cognitive status* made out of shared intersubjective expectations. The process and the context of communication, where those expectations are shared, are not given and determined in advance. On the contrary, they are fashioned by a dynamic dimension, since they influence, reflexively, each other.

During this form of communication (*i.e.*, a trust relation), both trustors and trustees are progressively brought to reveal themselves. They fill their identities with meaning through their trustful relations, and this meaning (as every meaning) is contingent upon the context of communication in which it occurs. Placed against the backdrop of communication, trust is not only the way we can provide the parties of the trust relation with meaning (reduction of uncertainty), but it is also the way we can co-construct the context of communication in which that meaning will be appraised and understood (systemic reduction of uncertainty). In philosophical terms, trusting is not only aimed at entering into relation with another person but also at seeing *who* the other person is, which is always a necessary step, in order to recognize *who* we are.

This means that the trustful relations of communication, where we decide to enter and where thereafter we are embedded in, participate in the construction of our personal identity. Trust is peculiar in what it enables us to give shape both to social relations and to the context of communication in which those relations are appraised and understood. By means of trust we can construct our personal identity in the sense that we delimit the sphere of what we can expect from others and of what others can accordingly expect from us, by structuring the conditions in which those expectations can be shared and evaluated. Since most human problems are problems of communication and control, as Norbert Wiener [15] has taught us, trust is also affected by problems of communication and control.

As remarked, trusting is a complex act that joins together what is subject to evaluation and calculation (trustworthiness) and what remains beyond control (the otherness of someone else's behavior): trusting never involves a choice between control and lack of control, but always both of

them at the same time. Trust involves a risk that can endanger our identity construction for three main raisons: it requires us to disclose and to expose ourselves to others (people cannot be prevented from being sources of information); it seems to establish an opt in/out regime for the use of personal data (dissent should be explicit, while consent is presumed); the information disclosed in a specific, trustful context of communication can be easily disembedded and re-contextualized. This is the reason why trust is meant to be at variance with privacy. It is time, therefore, to focus our attention upon the issue of privacy.

3. Privacy

In the past, the idea of privacy has been closely based on the notion of space. In the legal doctrine of privacy, this idea of space has always been thought of through the opposition between a *private* and a *public* sphere. From a philosophical standpoint, such opposition, still at play in some interpretations of privacy, could be misleading if not properly understood. The space of privacy is not shaped by a given content, that is, by a determined set of data that would belong to a private sphere. A set of data is not to be defined private because they would belong, ontologically, to a private space. The space of privacy is fashioned by the human power to refer something (*i.e.*, a set of data) to a unique point of reference. We do not understand much about privacy if we do not recognize in its construction the human attempt to pave a way towards *uniqueness*, *i.e.*, the regime of insubstitutability, by using materials that belong to the domain of homogeneity, *i.e.*, the regime of substitutability [16].

In other words, what can distinguish the public from the private sphere of life is not a different content (a peculiar type of data), but a different reference of the same content to a specific point of reference: the Self (both a source and a sum of information). The so-called "private" dimension (sphere, space or data) is referred to a point to which there is not the same reference in the public. It is this power to refer to the Self as a unique point of reference which explains privacy, rather than the simple delimitation of a more restricted domain within a wider space. This means that the protection of privacy is not viewed, in this perspective, as the protection of a delimited space (however such space is conceived: the house, the person, the body, the personal data, *etc.*) to be interdicted. On the contrary, the protection of privacy requires us to preserve a human capacity to act, that is, our capability to refer something to ourselves: *i.e.*, the power of self-identification, which is part of the human relations in the sense that it is both an individual and a relational activity, namely, an activity that we never achieve, entirely, by ourselves.

Philosophically, this implies that there are no data, *per se*, which are ontologically private or public. There are no private data that cannot be turned into public and vice versa. The private and the public worlds, which are ontologically coextensive, do not exist by themselves but, on the contrary, they are the corollary of a human activity. For that reason, people are constantly troubled with tracing the mobile, unsettled line between the private and the public. What is crucial to understand is that this activity does not consist, nowadays, in isolating the individuals from the society but, on the contrary, in placing them inside it. The space of informational privacy is the space in which we project and construct our own personality: this activity, however, never occurs in a void but necessarily inside society. This is the reason why, if our personality is made out of the sum of information concerning us, we have also to realize that this is not a static but a dynamic account of who we are. In fact, the space

of privacy is not constituted only by that amount of information. Rather, the space of privacy is given by the contexts of communication connecting us to the rest of society in terms of negotiated identities. In such contexts, to trace the line between the private and the public sphere of life is a matter of power.

People seem to take the definition of power for granted. They tend to associate power with some capability of acting, deciding or having influence over someone else's will, and they reduce it accordingly to large availability of money or to great means. Many associate power more directly with violence, force or, at best, with authority. Others associate power, in a more sophisticated way, with the ability to persuade or to produce the relevant information upon which people take decisions or behave. Few have a gnoseological conception of power. In this philosophical perspective that goes from Heidegger [17] to Foucault [18,19], power is also a means of self-knowledge: human relations are relations of power aimed to devise who we are. From this standpoint, we do not only make use of knowledge as a form of power. We also make use of power as a form of knowledge: what I am depends on what I *am capable* of doing both as regards to myself and to others. In this sense, it is not my identity that brings about my capacities. Rather, my capacities determine my identity.

We understand thus why privacy, understood as a way of constructing our personality, is viewed in our perspective as a *power* to refer something to a unique point of reference (a form of *empowerment of the Self*). We realize also why this power is always competitive, polemic, since the relation with others can represent an intrinsic *limit* to my power of self-construction. The process of referring data to one's account is not in fact an activity the subject can achieve by themselves. Our identity has always been made out of data that come from multiple and distributed sources, and often from sources that are potentially conflicting with each other. At all times, there is also a plurality of interpretation of those personal data (which co-construct the identity of individuals), and there is often a competition among these different sources of interpretation of personal data, according to the diverse contexts of communication in which those data are selected. However, this competition is not what threatens privacy but what makes privacy possible as a meaningful construction of human personality, since the meaning of data necessarily grows out of a "group phenomenon", that is, a collective process of communication embedded in some specific contexts.

However paradoxical it may be, through, the *commonly* shared reference to a unique point of reference, we can delineate what is personal from what is impersonal. We never accomplish it by ourselves, since any reference must be shared, in order to be meaningful: there are no private linguistic games. Hence, the space of privacy is also a context of communication. This notation is crucial to us since it connects privacy and trust, when understood as constructions of personal identity. The data we refer to ourselves have to be conceived as meaningful pieces of a personal history that must be, nevertheless, interpreted and understood in a shared context of communication. *The power to refer data to the self entails, thus, a society and a bundle of human relations*. This means that the individual power to trace the difference between private and public communications is already the sign of the existence of the (real or virtual) community defining the shared context of meaning where such communications can be interpreted and understood.

To protect privacy, *i.e.*, to construct a personal identity, is to protect this power of self-identification, which, however, always exists within the relation of mutual implication between me and others in a determined context of communication. The power of self-identification is confronted with the power of

being identified by someone else. Self-identification cannot be defended as a prerogative of an absolute subject (like for the Cartesian subject) that would be able to construct its identity in the blank, but only in the endless communication with others. In this perspective, the right to privacy is endowed with a double content: a *positive content*, *i.e.*, the power to refer data to a unique point of reference, and a *negative content*, *i.e.*, the power to rectify false/incorrect information, to have this information erased, and to prevent people from abusing of someone else's personal data. As we will see it in the last part of the paper, adolescents tend to understand privacy with regard to its positive content (as a construction of personality), while they happen to underestimate or to be not fully aware of its negative content (as a protection of personal data). Furthermore, the dialectics between the positive and the negative content of privacy strengthens at least three problems that are able to threaten the individual right to construct a personal identity in the Information Society, where the informational representation of human identity consists exactly of a set of "data that stem from multiple, distributed sources, in addition to traditional centralized storage devices" [20]. We have to focus our attention on these three problems.

3.1. Exportation vs. *Importation of Personal Data*

We have to remark that the question of privacy can no longer be confined to the risk of the exportation of data from the personal towards the public domain. On the contrary, the problem of privacy concerns more and more the risk of importation of data within the domain of the self by the multiple, distributed sources that can "speak" on behalf of us. We refer to all cases in which the power to mine, collect and distribute data can give an account of ourselves. In the Society of Surveillance [21], this goes up to the point that individuals can no longer keep a secret from others, since, because of the importation of data, they can learn about themselves what they could not have known before. This form of reference can be either concrete or abstract. It is concrete when people substitute us in the identity construction by referring to us data that detail our personality. It is abstract when people aggregate data by creating abstract profiles (for instance, statistical but not only), within which we are entirely or partly subsumed [22]. This can be achieved also without human intervention, by means of software agents or autonomic systems [16]. In this case, the process of self-identification is accomplished by means of an automated importation of data, which no longer requires a relation between me and others. In this case, the automatic importation of data displaces any shared construction of a context of communication. Here, the construction of identity cannot reconcile trust and privacy, because that impersonal construction no longer depends on the joint elaboration of a trustful context of communication that people could share as the horizon of meaning where their narrative identities can be interpreted and understood.

3.2. Explicit vs. *Implicit Communication of Personal Data*

Cognitive sciences and political philosophy remind us, from different standpoints, that, in our Society of Information, attention is becoming more and more a crucial issue [23]. The overload of information makes it decisive to select the relevant information to which we have to pay attention [24]. Attention to the information is a key question as regards to privacy, since the level of protection we expect for our privacy in a context of communication is correlated to the level of attention we pay to the information we disclose in it. The higher the attention we pay to the information disclosed, the

higher the level of protection we expect for that information. Cognitive attention is a scalable phenomenon, graduated according to the interest we have for the information disclosed or, more properly, to the emotions we attach to that information. In this perspective, the information concerning us deserves, normally, more attention than the information concerning others. People are thus likely to be more concerned with privacy when they disclose information about themselves rather than when they disclose information about others. Of course, this is quite *counterintuitive*, since the probability of violating privacy is higher when we disclose information about others. This is an elementary cognitive reason why we should pay greater attention to the information disclosed about others. What is more, things become more intricate, from a cognitive standpoint, if we replace the distinction between information about us and about others with the distinction between explicit and implicit communication of information. In fact, it is not simple to perceive what is implicit ("not-said") in what we communicate: frequently people speak about others through what they say about themselves. People do not pay the same attention to what is explicit and to what is implicit in their communication, since the "not-said" is the result of an hermeneutical comprehension of what has been said, the meaning of which depends on the context of interpretation of those who make the implicit communication explicit. As we will see later on, this is one of the problems of the youth's communication by social networking, since young people trust in the information disclosed, the interpretation of which can, however, bring to light what remains just implicit in their communications (thus resulting in a privacy violation).

3.3. Space vs. *Time Conditions in the Communication of Personal Data*

It has often been said that, in western societies, we live more and more in an *eternal present*. The speed of life, the pace of technological development [25] and the pretended *end of history* [26] force us to focus our attention only upon the present time: all these factors seem to out-shadow the depth of past and the indeterminate future. This cultural attitude has important consequences over the issue of privacy. In fact, people (and young people in particular) are brought to undervalue the consequences of their decisions in the long term. In particular, they can underrate the effects of their implicit consent to the disclosure and use of personal information, since they do not always perceive that such information will be evaluated, across time, within different contexts of interpretation. In the Society of Information, the contextual integrity and the coherence in the construction of identity is more subjected to menaces that come from the future rather than to menaces that come from the outside. The right to be forgotten is, intrinsically and hermeneutically, put into risk by the idea that past and future are just derived forms of temporality, when confronted to the reality of the present time. The right to be forgotten is logically endangered, if the idea of the eternal present becomes the *norm* that structures the interpretation of our personal communications. This hermeneutical canon is indeed at variance with the legal construction of privacy as a right of personality, which is not subjected to the passage of time. The level of privacy protection will be framed by the competition between the consent, implicitly given in the present and "for" the present, and the endless right of personality. Needless to say that also the interpretation of the different contexts of communication, where a relation of trust can take place across time, is displaced or endangered by the hermeneutical doctrine of an eternal present.

These problems about privacy tend to show that the identity construction in the Society of Information always grows out of a competition between different sources of data. In the following paragraph, we have to explain why this competition is, actually, intrinsic to any construction of personal identity and why it can represent, despite the problems outlined, the *locus* where trust and privacy can be, at least to some extent, reconciled.

4. The Construction of Personal Identity

In the age of information, the construction of personal identity is achieved by means of narration. In other terms, personal identity is made up of information (out of the distinction between offline and online) [1], which is provided with meaning through a coherent narrative construction of personal identity in a shared context of communication. The construction of personal identity is a polemic activity [16]. This competitive dimension becomes evident when the notion of identity is related to that of narration. Narration is, in its formal structure, the expression of a conflict that marks the passage of time. In this perspective, Arnaldo Momigliano, the great historian, affirmed that war has always been the main topic of the historical tale [27]. Needless to say, in addition, that even the philosophical identity of becoming is polemic in its nature, because expressed by the continuous passage between *being* and *non-being*, which is by itself warlike. The competitive construction of a personal narrative identity can be outlined by means of a mental experiment concerning autobiography, which we have expounded elsewhere [16] and we can briefly recall here.

Imagine two persons that are invited to write about the personal history of just one of them. The first one is invited to write an autobiography, whereas the second is invited to write a biography. They are both confronted with the same objects, a set of personal data. Unlike the improbable situation in which they write the same tale, they are likely to produce two stories that differ from each other on several points. Hence, the two accounts of the same life are in competition: they both seek to be considered the best account of what has been narrated. Furthermore, this competition is not necessarily biased in favor of autobiography, since there is no reason in principle to make it prevail over biography as the best account of the narrated self. Concerning that account, we may discern two narrating selves:

The *autobiographical Self* that stems from the process of self-reference. Autobiography is a narrative scheme that seems to reassure us, since it gives us the idea that the whole process of referring personal data to ourselves (collection and communication) is under our control. As we will see it, autobiography is also a competitive form of narration that entails a risk requiring from us a certain degree of trust;

The *competitive Self* that stems from the process of hetero-reference. Biography is a narrative scheme that does not reassure us, since it tells us that the identity construction is always negotiated, *i.e.*, it is at all times the outcome of a dialectics between me and others. This tension requires us to construct a trustful context of communication, where our narrative identities can be interpreted and understood.

In this case, the identity of the narrated self grows out of the competition between the two tales and, hence, between the two selves that we might wish to reconcile. For this reason, the personal identity of the narrated self is able to emerge when two conditions are met: firstly, when the competition is *fair*,

i.e., both the autobiographical and the competitive self are given at least equal opportunities in narrating the true story of the self; secondly, when the competition occurs in a shared context of communication.

Consider now the different case in which just one person is invited to write about her personal history: the case of autobiography (this case is not absorbed by the previous case, since in this circumstance the readers are not confronted by a double account of the self). The identity of the narrated self is yet again constituted by a set of data that derives, necessarily, from a selection of data. This selection is by itself significant, because the author has to choose the most relevant and trustworthy personal data, in order to give a meaningful and trustful account of the self. Of course, the omission is symmetrically significant, since also the omitted data give shape, in negative terms, to the self. From a hermeneutical or psychoanalytical standpoint, what is omitted may be, actually, more significant than what is selected. Also in this case, we can discern two narrating instances of the same Self:

An *autobiographical Self*, whose tale is significant for what the author chooses to select and to narrate: the set of relevant and reliable information. The author is inevitably concerned with tracing a sharp line between what data have to remain private and what data can become public.

A *competitive Self*, implied in the *autobiographical Self*, whose negative tale is significant for what the author excludes. The narrating instance of the competitive self is driven by strong forces, which are not always entirely governed by the author. Often, these forces are at play to prevent people from narrating what is most painful or harmful in their personal history. As we will see below, young people in particular tend to reveal only what they consider *harmless* to them. In this respect, what they narrate is a patchy, variable map of their relative certainties and fragilities, whilst their competitive self prevents them from reporting what can really endangers the integrity and the consistency of their self-narration.

A competition in fact is at play between the autobiographical and the competitive self, since one story cannot be simply reduced to the other. The identity of the narrated self grows out of the competition between two selves or two instances of the same self. This means that both in the first case, concerning the structure of intersubjectivity, and in the second case, concerning the structure of subjectivity, the identity of the narrated self is always *polemic*, since it emerges out of the struggle between *competing instances* of the self. Nevertheless, this competition is not a blind dispute but implies a communication. It entails both communicating with *others* (intersubjectivity: [28-30]) and communicating with *the other* that inhabits each of us (subjectivity: [31-33]). Here lies my point: even when people speak about themselves (*i.e.*, disclose personal data), they are involved in the construction of a trustful and shared context of communication, where their narrative identity is expected to be interpreted. This means that not only epistemic trust (*i.e.*, to trust that) but also relational trust (*i.e.*, to trust in) are deeply and necessarily intertwined with privacy in the identity construction, since the semantic understanding of data requires a society and a bundle of human relations.

The construction of personal identity is, accordingly, a competitive activity, with regard to privacy. As Vittorio Mathieu points it out, "privacy does not constitute an object but a relation, which cannot at its turn be objectified, of an object with an origin and an intention […]. In other words, privacy is, as well as law, a protection of freedom, but as *freedom of* and not only as *freedom from*" [34]. For this

reason, the violation of privacy is not the violation of an inner self that would be deprived of personal data or of the control thereof. A violation of privacy deprives the self essentially of a capacity, that is the active power to *take the initiative* of referring a content to the Self [22,34], namely, of developing a coherent story. The tactics of privacy is no longer defensive but goes to the point of constructivism, included the construction of a shared context of communication, which becomes more feasible in a world in which a context is conceived in informational terms. This power is thought of in the horizon of the autonomy of the Self, but is neither exclusive nor uncontroversial, since the identity construction, irreducibly grows out of both a *trustful cooperation* and a *competitive narration*.

This means also that the identity of the narrated self and thus the relation between trust and privacy are well founded and assured inasmuch as the relation between cooperation and competition is fair, *i.e.*, the narration of the self is given by both cooperative and competing instances according to *fair conditions*. Cooperation (*i.e.*, the mutual and trustful construction of a context of communication) and competition (*i.e.*, the polemic narration of personal identity) between different agents and instances (e.g., between different sources of data) can never be wholly excluded because they are inherent to the construction of the self. What matters is that that construction is based on fair, reciprocal conditions, and on the setting of a shared context of communication between those instances.

This brings about two consequences. Firstly, fairness is included among the philosophical premises of privacy, along with autonomy and dignity. The impact and the design of ICTs, the evolution of which can alter the conditions of cooperation and competition, are to be evaluated in relation to their potential *standings of fairness*, *i.e.*, their procedural capacities to comply with the conditions of a fair cooperation and competition in the disclosure of information. The minimal condition of fairness is assured when all instances are given at least equal opportunities to shape a true account of the Self. Secondly, fairness is displaced when people do not have a grip upon the conditions of the technological communication, which in turn has a tight hold upon them. The relation of mutual implication, according to which "if I make technologies; they, in turn, make me" [35] should not be eliminated. A fair and balanced relation between trust and privacy is assured not only when agents can technologically protect their identities but, primarily, when they participate in the construction of the ethical backdrop of the *value-sensitive* information technologies. In other terms, it is true that the evaluation of the design of ICTs requires us to unfold the values (the standings of fairness) imbedded in the design. However, such values cannot be really appraised and given meaning if we do not co-construct a trustful context of communication, where the meaning of those values can be interpreted and understood.

5. The Case of Social Networks: Facebook

In the present paragraph we do not propose an empirical survey on the use of Facebook and its related problems. We construct our argument on the basis of some empirical studies on the subject and we try to understand some of their results in the light of what has been said in the present essay. Among these studies, the analysis displayed by Danah Boyd deserves special attention as regards to the networked affordances of social networks sites "that shape how people engage with these environments" [36]. Afterwards, we recall some of our previous considerations and measure their soundness in relation to the case of Facebook.

Danah Boyd develops the pivotal notion of "networked publics" that is to some extent complementary to our analysis of the networked construction of identity within a "context of communication", that is an informational space structured by the tension between trust and privacy. "*Networks publics* are publics that are restructured by networked technologies. As such, they are simultaneously (1) the space constructed through networked technologies and (2) the imagined collective that emerges as a result of the intersection of people, technology, and practice" [36]. The idea that networked publics are both a space and an imagined collective is very perspicuous and interesting: it explains the complex dynamics according to which the networked affordances of the architecture of a particular environment enables people to develop an image of themselves that is projected, understood and evaluated within the space constructed – in informational terms – by the interactions among users. Danah Boyd explains well how this dynamics is structured: "Networks publics' affordances do not dictate participants' behavior, but they do configure the environment in a way that shapes participants' engagement. In essence, the architecture of a particular environment matters and the architecture of networked publics is shaped by their affordances" [36].

Danah Boyd is very clear in her analysis and we will take advantage of her analysis of the networked affordances of social networks sites that easily apply to the case of Facebook. However, we would like to briefly bring up a point that seems of great interest, even if it will be impossible to deal with it in full here. Networked affordances enable but "do not dictate participants' behaviors". This explains why participants *can* behave in a certain way in some specific environments but does not actually explain why they *do* behave in such way. The easiest way to deal with it would be to state that technological affordances let humans be free whether or not to endorse the possibilities they afford. In this perspective, the relation between technological affordances and actual behaviors would be only a probabilistic one. Even if we subscribe the idea that this relation is a non-deterministic one, we believe that people–knowingly or unknowingly–endorse possibilities enabled by technological affordances, when such endorsement gives them new "powers" [24], which are connected with their own desires. In the case of social networks, notably young people are given the possibility (and therefore the power) to co-construct, in informational terms, a meaningful "context of communication", where their narrative identities can be formed, enacted and evaluated, even if this informational context can easily collide with the different empirical contexts that people belong in real life and are also represented online: this collision is a direct expression of the informational tension that exists between trust and privacy. Such informational dimension is clearly grasped by Danah Boyd when she underlines that "the properties of bits regulate the structure of networked publics, which, in turn introduces new possible practices and shapes the interactions that take place" [36].

Having in mind our general remark on the point, it is useful to see what are, according to Danah Boyle, the features of social networks sites that function as technological affordances. There are four such features: "profiles, Friends lists, public commenting tools, and stream-based updates" [36]. Let us briefly summarize what Danah Boyle says for each of those features, in order to connect them to our previous analysis:

a) *Public or semi-public profiles*: "profiles are a place where people gather to converse and share. Conversations happen on profiles and a person's profile reflects their engagement with the site. As a result, participants do not have complete control over their self-representation" [36]. This

consideration is crucial and applies to what remarked in the fourth paragraph as regards to the competitive construction of personal identity. This feature is a chief character of Facebook's communication, which is backed by three more specific elements that delineate Facebook from other social networks: (1) Facebook requires users, in principle, to give their true identity (which, however, allows the possibility for users to adopt a *pseudonymous* or an *eteronymous*. It would be interesting to distinguish between the two types of profiles: the first one is the case of someone who wants to conceal his/her true identity, whereas the other is the case of someone who wants to have his/her identity to coexist with another fictive identity); (2) Facebook is meant to offer an extended level of customization that enables users to knowingly and creatively craft their profiles and to set the limits of their visibility (in relation to what and to whom is displayed), in order to reach a truly public or a semi-public audience [36]; (3) Facebook allows users to construct their own profiles using "plain text", which is a lowest common denominator assuring independence from specific programs of encoding or formatting;

b) *Friends list*: "on social network sites, participants articulate who they wish to connect with and confirm ties to those who wish to connect with them" [36]. Danah Boyd interprets this feature as a way to articulate an "intended public" that defines the site of communication in terms of an homogeneous or heterogeneous social context (the former being characterized by ties to those already belonging to our social context and the latter by ties to those belonging to "different" social contexts). This interpretation applies to Facebook and is consistent with our conception of social ties (expounded in the third paragraph) understood in terms of trust relations intended to widen or narrow the sphere of our social context of communication. There is a further point to be stressed that is connected with people's activism in shaping the context of communication and where they decide to project their identities: to "confirm" ties gives them a flavor of voluntarism (in terms of expressed choice) that seems to be absent or just implicit in offline human connections. This aspect is even quantifiable in social networks as Facebook and becomes a synonymous of our popularity and scalability (that is the "potential visibility" [36] of our contents on a large scale).

c) *Tools for public communication*: "most social network sites provide various tools to support public or semi-public interactions between participants. Group features allow participants to gather around shared interests" [36]. In that respect, Facebook displays several tools with which users may interact: 1) the *Wall*, that is a space on the user's profile page where friends can post messages and comments on the profile for the user to be seen and commented on; 2) *Photos*, that is a tool by means of which users can upload photos (which happen to raise privacy issues in what they may convey about other friends or persons in general and for what concerns the metadata of a photo); 3) *Pokes*, that enables users to send each other a notification (a virtual poke) that tells users that they have been "poked", that is to say that they have been alerted that other users would like to have access to the user's profile page. All the mentioned interacting tools are means through which users can articulate the relation between privacy issues and trust relations. In fact, on the one hand, tools for public communication and interaction function on the basis of previously determined privacy settings; on the other, they can ease the formation of

trust relations since they allow users to gather around "shared interests": as mentioned elsewhere [10], one of the key element of trustworthiness is parties' shared concern for common interests or goals.

d) *Stream-based updates*: "status updates" is a tool that "allow participants to broadcast content to Friends on the sites" [36]. Friends are informed, in this way, about users' actions, whereabouts, messages or comments. Updates can be, in some cases, re-displayed on a user's profile page for other users to comment on. We would like to highlight some comments offered on this point by Danah Boyd: "in doing so, participants get the sense of the public constructed by those with whom they connect" [36] and, more broadly, "social networks sites are publics both because of the ways in which they connect people en masse and because of the space they provide for interactions and information" [36]. These comments are crucial in order to understand three key points: (1) the notion of personal identity displayed by social networks is no longer concerned with the description of who we are but rather with the progressive construction and updating of who we would like to be: it falls upon us to decide what (including who) we want to select and what (including who) we want to give up; (2) this construction is a co-construction that expresses the tension between what we want to include (trust) and what we want to exclude (privacy) by our social context of communication; (3) this co-construction is shaped by networked affordances in the sense that technologies are no longer perceived as means directed towards determined ends but as an environment, *i.e.*, a space to inhabit, whose structural properties based on information (bits, data, etc.) differ from those of the physical space based on things (atoms, objects, etc.).

These technological affordances thus shape the environment where the online construction of personal identity by means of social networking grows out of the tension between trust (openness and inclusion) and privacy (closeness and exclusion). Against the backdrop of what we have noticed so far by summarizing Danah Boyd's interpretation of social networks, we can now recall in five points the nature of the trade-off between trust and privacy as the framework of the online identity construction. After this framework is sketched out, we will measure to what extent the general interpretation of social networks' features and the analyzed trade-off between trust and privacy applies to the specific case of Facebook.

5.1. The Trade-off between Trust and Privacy

1. Trust and privacy are, *prima facie*, at variance with each other, because trust seems to involve a certain disclosure of personal information whereas privacy seems to involve a certain closure of personal information: there would be, thus, an irreducible trade-off between trust and privacy.
2. This trade-off relies on two undisclosed premises that have to be made more precise. Trust is not only concerned with the communication of personal data but, above all, with the construction of a trustful atmosphere and a web of relations. The protection of privacy is not a passive attitude concerned with the delimitation of a private space but, on the contrary, it is an active dimension concerned with taking the initiative of referring data to a personal account across time.
3. Trust and privacy are different sides of the same coin: they are both involved in the construction of identity. Trust aims at the elaboration of a specific space (a shared context of communication

where to include others) where the self-narration can be interpreted, appraised and understood. Privacy is concerned with the elaboration of a specific time, in which the integrity and coherence of the narrative identity is assured across time (this implies excluding others from our narration). This is likely to be the possible cultural danger of some social network sites, like Facebook, that in a sense strengthen the dichotomy between inclusion and exclusion.

4. The identity construction is put at risk and endangered by: (a) the (automated) importation of data that pierces the context of communication from the outside and causes danger to the contextual integrity of self-narration (also because of the "replicability" and "searchability" of networked content [36]); (b) the implicit communication of someone else's personal data that pierces the context of communication from the inside and alters the contextual integrity of someone else's narration (also because of the "persistence" and "scalability" of networked content [36)]; (c) the understanding of time as an eternal present that endangers both the coherence of the narration of personal identity across time and the right to be forgotten (which is the legitimate counterpart of the persistence of online data automatically recorded and archived);
5. The construction of online personal identity is a complex process in which trust and privacy can be reconciled to the extent to which cooperation and competition between narrating instances of the Self are balanced according to standings of fairness. Those standings cannot be simply and automatically embedded in the technological solutions afforded by design and architecture but they need to be construed and evaluated according to a shared context of communication, which requires users also to share a common horizon of meaning. Behaviors can be, thus, facilitated or discouraged by technological settings but the interpretation of behaviors and the concrete choice of technological settings is still guided by the mental attitude to give meaning to specific notions as trust, privacy, identity and so forth.

After these remarks, we can focus now our attention at the ways youth in particular (but not only) deal with trust and privacy notions and issues in the co-construction of online personal identity through the use of a social network like Facebook.

5.2 The Meaning of Youth for Digital Natives

First of all, empirical studies tend to mold the interpretation of the use of social networks, especially in relation to the issue of privacy, according to the different ages of users [37-39]. This is correct, and a necessary methodological starting point for two main reasons: (1) different ages bring about different levels of maturity and self-awareness along with different patterns of social and psychological needs; (2) the evaluation of the protection of privacy rights is linked to the explicit or implicit consent to the treatment of personal data, which depends on the major age. However, this approach seems to let apart or to out-shadows what is the key aspect of the problem: how young people implicitly interpret the definition of "youth". For digital natives, the use of ICTs, especially social networks, is a distributed, collective *self-interpretation* of what "youth" is and means in the Society of Information. This self-interpretation stems from the detailed empirical studies over the teens' use of Facebook, if read from this standpoint. "Youth" is "participation". Participation is not to be understood according to the distinction between passive destination of information and active creation of content. It is not a mere

synonymous of user-generated content, at least not when this expression is literally and reductively understood as meaning that content is created by an author. If such expression is correctly understood (as in [40]), it gives us a clue to understanding the meaning of participation. The networked generation of content is not a private, individual activity but a "group phenomenon" [40], according to which teens create contents which are already directed to someone else: there is always an "expected audience" [41] or "networked publics" [36]. Young people implicitly seem to know that meaning is a function of a context. For this reason, as digital natives, teens tend to interpret youth as a shared participation in the construction of the *context of communication* ("youth") in which they expect that their narrative identities will be meaningfully experienced, interpreted and understood. They wish to produce a web of trustful relations with their "expected audience" or "networked publics" (we have already remarked in this respect that this form of participation, this web of relations, can hide a dynamics that is ultimately based on the relation between inclusion and exclusion). This leads us to a second central point.

5.3. The Co-construction of the Informational Context of Communication

Social networks, like Facebook, are technological platforms where people experience a new form of communication, by strengthening previous ties or creating new ones, in order to sort out the sense of anonymity that has characterized the industrial society and still affects the information society. In this way, people, and young people in particular, tend to construct their online personal identity or at least to provide themselves with a re-appropriated sense of the Self. Of course, this entails a communication of personal data according to the structural affordances of online communication, which are based on the properties of "bits" instead of those of "atoms" [36]. What are those specific structural affordances and thus what are the specific features of such communication?

We have already made reference to those structural affordances but we briefly recall them here, as formulated by Danah Boyd, who believes they emerge out of the properties of bits [36]:

1) *Persistence:* online expressions are automatically recorded and archived.
2) *Replicability*: content made out of bits can be duplicated.
3) *Scalability*: the potential visibility of content in networked publics is great.
4) *Searchability*: content in networked publics can accessed through search.

This explains, in terms of structural affordances, a point which we have insisted on from the beginning: in the digital reality the construction of a text is not an activity truly separated from the construction of a context since both of them are made of bits that are characterized by the same structural affordances. The identity of those entering into communication grows out of the process of communication and it is part of the context of communication people jointly elaborate thanks to those structural affordances. In that sense, social networks are "contexts of communication" in which young people tend to form their identity more than contexts in which they communicate on the basis of an already established identity. What is innovative is that both identity and context are made out of a sum of information. Identity is a sum of information that gives content to the narration of the Self, whereas context is made out of a sum of information that characterizes a specific situation [2]. It is the informational nature of the context of communication that represents the originality of such form of

communication. This originality is, thus, both hermeneutical (in terms of informational contexts) and technological (in terms of networked and structural affordances emerging out of the properties of bits). When communicating through social networks, young people do not only aim to bridge the discrepancy between the ideal and the actual self [42], but they implicitly and, to some extent, unknowingly co-construct their identities and the context of communication where such identities will be interpreted and understood. Similarly, Boyd remarks that "knowing one's audience matters when trying to determine what is socially appropriate to say or what will be understood by those listening. In other words, audience is critical to context" [36].

The disclosure of information young people accomplishes in the social networks is therefore aimed both at constructing "their" online identities and setting "their" shared context of communication in which such information is, normatively, to be comprehended and evaluated. This can lead teens to restrict their "social network profile to private, making it inaccessible to anyone outside their group of friends" ([43] that also refer to [37,44]). If we look to this phenomenon from this point of view, *i.e.*, the effort to create a sphere of life where to be understood and validated by their peers, we understand why young people, according to their psychological needs, may or may not change their privacy settings (there is in fact evidence, in the literature, in both directions: see [43]). In other terms, for the first time, young people are given the possibility to co-construct the contexts of communication, *i.e.*, the "horizon of meaning" [11], in which their self-narrations are given meaning. And they can do that in a ground-breaking way, since both the narrated identities and the context of communication are made out of the same malleable materials: information (made out of data made out of bits). "The computational rendition of reality has far-reaching implications in the sense of recapturing a growing proportion of the physical and cognitive landscape of contemporary life into the medium of permutable and recombinable information" [45]. Teens trust in social networks, like Facebook, because they are mutually involved in the elaboration of their context of communication made out of the "liquid" digital information characterizing the specific situation in which they interact by social networking: with of course all the problems that go along with the possibility of re-contextualization of such information (*i.e.*, the collision of contexts underlined also by Danah Boyd [36]). In this, way trust plays a decisive and complex role in the analysis of social networks, and this leads us to a third point.

5.4. The Risks of Systemic Trust and Familiarity

Young people's trust, displayed in social networks, is not only a form of personal trust that depends on an intersubjective act of delegation. Rather, it is a form of systemic trust [9] that is concerned with a set of generalized expectations of stability towards a world or, in our own terms, towards a certain context of communication. The web of trustful relations (*i.e.*, teens' mutual expectations) fill this world with an atmosphere of "familiarity" [9], which is recursive in the sense that it is a precondition for establishing further relations of trust. This brings about three consequences: (a) familiarity enables us to step out of our natural diffidence towards others, caused by the unpredictability of their future behaviors (their otherness). However, familiarity is capable of helping us overcome our diffidence, not because we get to know other users (which is true only in some cases), but since we share with them the same context that we have contributed to build: familiarity is the familiarity of the same world, and not of the same profiles. Online profiles are *poles of attraction* only because they are grasped and

interpreted within the same universe of meanings, symbols, references; (b) familiarity widens the scope of trust since it makes trust to become a distributed attribute of the system more than a punctual quality of personal relations. This means that familiarity has the tendency both to immunize the system from single delusions, *i.e.*, from single failures of trust relations, and to weaken the requirement of motivation, which is needed in order to establish a personal trustful relation [9]; (c) familiarity is apt to reinforce our trust in the system and thus to lessen our defense against specific aggressors: this is typical of all the regimes of inclusion, which makes us represent risks as something that comes from the outside. In contrast, it has been remarked, for instance by Helen Nissenbaum, that betrayals come "from those who are allowed within our spheres of safety, within our safe zones" [46].

As a result, systemic trust in social networks can expose adolescents to more risks, since it becomes less evident to them where risks come from. In a context built on systemic trust, it is easier to develop trustful relations but it becomes more difficult to have control over those relations, since who trusts in the system depends, eventually, on the complex functioning of the system as a whole, which makes it difficult to detect and to have power over single unpredicted behaviors. On the one hand, building a trustful context of communication reinforces trust and privacy as identity constructions, because it enables people to structure the context in which their identities are expected to be interpreted and understood. On the other, the systemic trust, which seems to be a mark of social networks, is likely to expose young people to uncalculated risks that endanger their privacy, understood as a form of control over personal information. This leads us to a further point concerning the idea of privacy.

5.5. The Co-construction of Personal Identity

Young people that use social networks, like Facebook, do not really (*i.e.*, knowingly) pursue a balance between trust and privacy. The trade-off between trust and privacy could be misleading for the reason already outlined: both trust and privacy, experienced in social networks, are concerned with the identity construction. Rather, teens pursue, implicitly, a balance between a traditional (based on settings and norms) and an informational idea of privacy (based on structural affordances): like adults, young people pay attention to disclosing information that construct their online personal identities, even if, unlike them, they are rather inclined to believe that privacy, understood as a legal institution aimed at protecting us from unwanted intrusions, is pretty outdated in the networked Society of Information. In this sense, there might be a trade-off between the construction of personal identity and the limitation over access to personal information: "Disclosure thereby becomes an aspect of identity construction, and that construction is linked with popularity: the people that are most popular are those whose identity construction is most actively participated in by others. As a result, the risks of limiting access to personal information become greater than the risks of disclosure, because, when limiting access, the individual also limits the potential for identity construction and thus reduces his or her popularity" [47]. It has also been remarked, nonetheless, that "there is no correlation between providing personal information online and a lack of concern for privacy" [43], and, in addition to this, "students instead managed audience concerns through privacy settings and obfuscating nicknames" [48]. The relation between disclosure and limitation over access to information seems, thus, to be more a question of self-perception than one of concern for privacy violations. This is the reason why we have insisted upon a socio-cognitive conception of trust, because it is crucial to understand how teens

perceive and represent the world, *i.e.*, the entrusted context of communication they live with and interact in. When the identity construction is concerned, not only adolescents need to entrust their peers, in order to share information with them as a "token of friendship and trust" [43], but, more fundamentally, they need to be trusted, that is, they need that their self-narration is integrated by that of their peers, who are crucial instances of the *competitive Self* (see paragraph 4). This is backed by several studies on social media [41,47,49,50], as it has been remarked: "since much of peer socializing among young people goes on via social media, young people's conduct, both offline and online, is shaped by a general desire to be validated by their peers" [43]. Teens perceive their world and the resulting collective self-perception "forged when people make judgments based upon the mosaic of information available about us" [51, see also 36], as the necessary outcome of a co-constructed identity in a shared context of communication. This leads us to consider a final point.

5.6. Accountability

The ways teens make use of social networks, like Facebook, tend to support our doubts (see paragraph 3.3) as to what threatens the construction of personal identity via social media. Firstly, "aggregation and analysis involving large databases are increasing the possibility that individual privacy may be invaded in new and more substantial ways" [43], because "personal information is not only outside our control but also subjected to a bureaucratic process that is itself not adequately controlled" [51]. Secondly, "it is common for people who live their lives mediated by digital technologies to disclose, *knowingly and unknowingly* [we underline], personal information online. Once digitized, such information is virtually irretrievable and may be intercepted or purchased by commercial entities, governments, or individuals for marketing or other sinister purposes" [43] that refer also to [51-53]. Thirdly, "scholars claim that young people will be the first to experience the aggregated effect of living a digital mediated life, with the corresponding creation of various identities and digital dossiers *over a long period of time* (we underline). Solove describes modern 'architectural problems' related to privacy, which involve 'the creation of a risk that a person will be harmed in the future'" [43]. Fourthly, "networks publics force everyday people to contend with environments in which contexts are regularly colliding. Even when the immediate audience might be understood, the potential audience can be far greater and from different contexts. Maintaining distinct contexts online is particularly tricky because of the persistent, replicable, searchable, and scalable nature of networked acts. People do try to segment contexts by discouraging unwanted audiences from participating or by trying to limit information to make searching more difficult or by using technologies that create partial walls through privacy settings" [36].

All these problems are different and, accordingly, they are not likely to be encountered in the same way. Each of them suggests a different solution that should be, nevertheless, understood as a part of a complete picture. This picture is dominated by the requirement of accountability. The first problem, concerning the automated collection and storage of data, suggests, according to [43], that "companies that collect and store personal information 'have an obligation to build secure systems, and they ought to be held *accountable* [we underline] under the law if they don't'". The second problem, as to the implicit communication of a third party's personal information, needs a solution based on education. However, education is not to be aimed at scaring teens away from social media [43,54,55], by

exaggerating the risks involved in the use of social networks. Education should be intended in a way that makes young people sensitive to what is implicit (not-said) in their communication: teens should be made more accountable to whom might be harmed by their disclosure of personal information, when the infringement of a third party's privacy is the unintended consequence of their self-narration. The third problem, regarding the effects of adolescents' actions across time (the disclosure of information and the implicit consent to the use of personal data), needs, however, a solution based on limiting their accountability. Young people deserve, like anybody else, a "right to be forgotten": they cannot be held accountable for what can emerge from a digital dossier "over a long period of time". They cannot be unfairly enchained to the past, once they have totally left the context of communication in which personal data have originally been disclosed. People should be made accountable towards other people because of the harm they have caused to them. They cannot be made unreasonably accountable to their own past: "'profiles on social networking sites won't always show up in a search engine query, but they will appear when members of those services track down the data subject' [56]. In the past, oral gossip could tarnish a reputation, but it would fade from memories over time. People could move elsewhere and start anew. Being shamed in cyberspace, however, is capable of becoming a 'digital scarlet letter' [51]" [43]. As observed, people should always be able to take the initiative of narrating their history, even if such narration is never made out of their exclusive creation [57]. The fourth issue is difficult to deal with, "because, with the audience invisible and the material persistent, it is often difficult to get a sense for what the context is or should be. […] In networked publics, contexts often collide such that the performer is unaware of audience from different contexts, magnifying the awkwardness and making adjustments impossible" [36]. This final remark is important since it enables us to stress that the online construction, segmentation and shaping of contexts are, on the one hand, a new and vital character of online communication and, on the other, are subject to the structural affordances that emerge out of the properties of bits and allow contexts to be pierced and collide each other both in space and across time.

6. Conclusions

The relation between trust and privacy is traversed by several contradictions. At a first glance, trust and privacy seems to necessarily entail a trade-off: for instance, young people share personal information on social networking because they already trust each other or in order to trust each other, with the result that they endanger their privacy and that of their peers. However, as understood from the standpoint of the identity construction, both trust and privacy point to the same end, even if in different manners. The concern for trust is directed at setting a context of communication, made up of trustful relations, in which young people's identities can be validated by other peers. The concern for privacy is aimed at suggesting what personal information it is fitting to reveal and to distribute in that context, by connecting the social expectations of privacy protection to the informational norms of contextual integrity [58], which are not previously fixed but depend on the sum of information that characterize a situation, *i.e.*, a social network, in terms of a trustful context of communication.

Creating a trustful context of communication requires social networks users to develop a *systemic trust*, in Luhmann's terms [9], or to create a *supra-agent*, in Floridi's terms [59], which is a union of agents that form a single unit based on confidentiality. This raises some problems, as already pointed

out, that depend on the systemic or supra-individual dimension of trust. From a technological standpoint, it has been correctly remarked that "it is extremely difficult for the average citizen to keep up with the pace of technological change" [43]. It is true that "few people would be knowledgeable enough about digital technologies to have an effective sense of what information they are sharing is publicly accessible and what is private" [60]. This means that people are more exposed than before to the "information risk" [61] that derives from the invisible dimension [62] of their digital operations. From the standpoint of confidentiality, the following consideration is significant: "Confidentiality is a bond that is hard and slow to forge properly, yet resilient to many external forces when finally in place, as the supra-agent is stronger than the constitutive agents themselves. (…) But it is also a bond very brittle and difficult to restore when it comes to betrayal, since the disclosure, deliberate or unintentional, of some personal information in violation of confidence can entirely destroy the privacy of the new, supra-agent born out of the joining agents, by painfully tearing them apart" [59].

More generally, teens' expectations of privacy protection or, to put it differently, teens' expectations of identity construction, which are set and developed in the shared and trustful contexts of communication they have cooperated to create by social networking, can be frustrated, since the information produced in those contexts can be easily disembedded and re-contextualized across time, because of the already mentioned collision of contexts and consequences of the structural affordances of the networked acts in terms of persistence, replicability, scalability and searchability. In this sense, the disaggregation of data, their "mobility, transferability and combinability" [45], is a structural feature of the digital fabric of the Internet reality. In fact, the pervasive use of information technology is challenging our traditional way of thinking about the world and our own identities in terms of stable and lasting structures, which are more and more reconstituted into novel social and individual forms. Young people, as digital natives, are likely to be more inclined to conceive the informational construction of personal identity as a competitive activity which is characterized by a specific and original dimension: both the identity and the context of which identity is part are formed by the permutable and recombinable information based on the paradigm of computation [45]. On the one hand, this enables people to mold their self-narration and the context of communication in which this narration is displayed. On the other, the transferability and the combinability of re-contextualized information is able to alter the meaning of their information, thus endangering the integrity of their self-narration.

In conclusion, the perspective we have chosen for analyzing the relation between trust and privacy, *i.e.*, the construction of personal identity, allows us to make a final, brief remark. This remark is concerned with the supposed transparency of the personal data displayed by social networking. As mentioned at the start of this paper, the meaning of the world "revelation" is twofold; the disclosure of data, at the same time reveals personal information (transparency) and hides the conditions of transparency (which never appear). In this sense, we have to observe that adolescents' concern for privacy includes, primarily, a strive for *privacy from adults*, from their surveillance. Parents should be aware of the fact that the *struggle* for the construction of personal identity (the polemic activity of the competing instances of the autobiographical Self, seen in paragraph four) is a constitutive ingredient of a personal identity, maybe the most important one, since it is the dimension in which young people recognize the patchy, relative map of their certainties and fragilities. However, this map is consigned to the written in a way that is always more selective than is usually expected. Secret diaries, both offline

and online, are most often governed by the capacity of the competitive Self to leave out of the narration what cannot be confessed to anyone, namely, what is both most painful and harmful. In other terms, even the most secret messages, are written, offline and online, *as if* they could be one day looked for and read by someone else. Parents who love to look in private diaries or to intrude in social networks will find out, quite often, only what is *already* waiting for them.

Acknowledgements

I would like to thank all the students of my seminars (November 2010), with whom I have been able to discuss some of the topics of this paper. Discussing with them over the ways digital natives think about and make use of social networks has been a source of inspiration and a taxing test for my ideas.

References

1. Floridi, L. A look into the future impact of ICT on our lives. *Inf. Soc.* **2007**, *23*, 59-64.
2. Dey, A.K. Understanding and using context. *Pers. Ubiquitous Comput. J.* **2001**, *5*, 4-7. Available online: www.cc.gatech.edu/fce/ctk/pubs/PeTe5-1.pdf (accessed on 3 August 2011).
3. Floridi, L. Information Ethics, its Nature and Scope. In *Moral Philosophy and Information Technology*; van den Hoven, J., Weckert, J., Eds.; Cambridge University Press: Cambridge, UK, 2008; pp. 40-65.
4. Floridi, L. The method of levels of abstraction. *Minds Mach.* **2008**, *18*, 303-329.
5. Durante, M. Re-designing the Role of Law in the Information Society: Mediating between the Real and the Virtual. In *Law and Technology. Looking into the Future*; Fernandez-Barrera, M., Gomes de Andrade, N., de Filippi, P., de Azevedo Cunha, M., Sartor, G., Casanovas, P., Eds.; European Press Academic Publishing: Firenze, Italy, 2009; pp. 31-50.
6. Sartor, G. Privacy, Reputation and Trust: Some Implications for Data Protection. In *EUI Working Paper*, Series Law 2006/4, European University Institute, 2006. Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=891123 (accessed on 3 August 2011).
7. Lévinas, E. *Totalité et infini. Essai sur l'extériorité*; M. Nijhoff: The Hague, The Netherland, 1961.
8. Gambetta, D. *Trust*; Basil Blackwell: Oxford, UK, 1990.
9. Luhmann, N. *Trust and Power*; John Wiley & Sons: New York, NY, USA, 1979; pp. 1-103.
10. Durante, M. What Model of Trust for Networked Cooperation? Online Social Trust in the Production of Common Goods (Knowledge Sharing). In *Living, Working and Learning Beyond Technology*; Bynum, T.W., Calzarossa, M., de Lotto, I., Rogerson, S., Eds.; University of Pavia: Mantua, Italy, 2008; pp. 211-223.
11. Gadamer, H.G. *Truth and Method [1960]*; Barden, G., Cumming, J., Trans.; The Seabury Press: New York, NY, USA, 1975.
12. Castelfranchi, C.; Falcone R. Social Trust: Cognitive Anatomy, Social Importance, Quantification and Dynamics. In *Proceedings of the first Workshop on Deception, Fraud and Trust in Agent Societies*, Minneapolis/St. Paul, MN, USA, 9–13 May 1998; pp. 35-49.
13. Castelfranchi, C.; Falcone, R. Trust Theory. 2007. Available online: http://www.istc.cnr.it/T3/trust (accessed on 3 August 2011).

14. Castelfranchi, C.; Falcone R. Socio-Cognitive Model of Trust: Basic Ingredients. 2008. Available online: http://www.istc.cnr.it/T3/trust (accessed on 3 August 2011).
15. Wiener, N. *Cybernetics: Or Control and Communication in the Animal and the Machine*; The MIT Press: Cambridge, MA, USA, 1948.
16. Durante, M. Rethinking Human Identity in the Age of Autonomic Computing: The Philosophical Idea of the Trace. In *The Philosophy of Law Meets the Philosophy of Technology: Autonomic Computing and Transformations of Human Agency*; Hildebrandt, M., Rouvroy, A., Eds.; Routledge: London, UK, 2011; pp. 85-103.
17. Heidegger, M. *Being and Time [1927]*; Macquarrie, J., Robinson, E., Trans.; Harper: London, UK, 2008.
18. Foucault, M. *Power/Knowledge: Selected Interviews and Other Writings, 1972–1977*; Gordon, C., Ed.; Pantheon: New York, NY, USA, 1980.
19. Foucault, M. *The Order of Things: An Archaeology of the Human Sciences*; Vintage: New York, NY USA, 1994.
20. Kephart, J.O.; Chess, D.M. The Vision of Autonomic Computing. In *Manifesto*; IEEE Society: Washington, DC, USA, 2003. Available online: http://www.research.ibm.com/autonomic/research/papers (accessed on 3 August 2011).
21. Lyon, D. *Surveillance Society: Monitoring Everyday Life*; Open University Press: Buckingham, UK, 2001.
22. Rouvroy, A. Governmentality in an Age of Autonomic Computing: Technology, Virtuality and Utopia. In *The Philosophy of Law Meets the Philosophy of Technology: Autonomic Computing and Transformations of Human Agency*; Hildebrandt, M.; Rouvroy, A., Eds.; Routledge: Oxford, UK, 2011, (forthcoming).
23. Castells, M. *Communication Power*; Oxford University Press: Oxford, UK, 2009.
24. Durante, M. Perché l'attuale discorso politico-pubblico fa leva sulla paura? *Filos. Polit.* **2010**, *1*, 49-70.
25. Virilio, P. *Speed and Politics: An Essay on Dromology*. Polizzotti, M., Trans.; Columbia University Press: New York, NY, USA, 1986.
26. Fukuyama, F. *The End of History and the Last Man*; Free Press: New York, NY, USA, 2006.
27. Momigliano, A. *The Classical Foundations of Modern Historiography*, Cambridge University Press: Cambridge, UK, 1992.
28. Ricoeur, P. *Soi-même Comme un Autre*; Seuil: Paris, France, 1996.
29. Ricoeur, P. *Parcours de la reconnaissance*; Editions Stock: Paris, France, 2004.
30. Davidson, D. *Subjective*, *Intersubjective, Objective*; Oxford University Press: Oxford, UK, 2001.
31. Lévinas, E. *Autrement qu'être ou au-delà de l'essence*; M. Nijhoff: The Hague, The Netherlands, 1974.
32. Lévinas, E. *Entre nous. Essai sur le Penser-à-l'autre*, Le livre de poche: Paris, France, 1998.
33. Kristeva, J. *Strangers to Ourselves*; Roudiez, L.S., Trans.; Columbia University Press: New York, NY, USA, 1994.
34. Mathieu, V. *Privacy e Dignità Dell'uomo. Una Teoria Della Persona*; Giappichelli: Torino, Italy, 2004.

35. Ihde, D. Postphenomenology—Again? In *Working Paper n. 3*; The Centre for STS Studies: Aarhus, Denmark, 2003.
36. Boyd, D. Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications. In *Networked Self: Identity, Community, and Culture on Social Network Sites*; Papacharissi Z., Ed.; Routledge: London, UK, 2010; pp. 39-58.
37. Lenhart, A.; Madden, M. *Teens, Privacy and Online Social Networks*. Pew Internet and American Life Project: Wasghinton, DC, USA, 2007.
38. Lwin, M.O.; Stanaland, A.J.; Miyazaki, A.D. Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *J. Retail.* **2008**, *84*, 205-217.
39. Steeves, V.; Webster, C. Closing the barn door: The effect of parental supervision on Canadian children's online privacy. *Bull. Sci. Technol. Soc.* **2008**, *28*, 4-19.
40. Shirky, C. *Here Comes Everybody. The Power of Organizing without Organizations*; Penguin: New York, NY, USA, 2008.
41. Boyd, D. Why Youth (Heart) Social Network Sites: The Role of Networked Publics. In *Youth, Identity and Digital Media*; Buckingham D., Ed.; MIT Press: Cambridge, MA, USA, 2007; pp. 119-142.
42. Higgins, E. Self-discrepancy: A theory relating self and affect. *Psychol. Rev.* **1987**, *94*, 319-340.
43. Marwick, A.E.; Diaz, D.M.; Palfrey, J. Youth, privacy and reputation (literature review). *Berkman Center Intern. Soc. Res. Publ. Ser.* **2010**, *5*, Available online: http://cyber.law.harvard.edu/publications/2010/Youth_Privacy_Reputation_Lit_Review (accessed on 3 August 2011).
44. Hinduja, S.; Patchin, J.W. Personal informat*ion of adolescents on the Internet: A quantitative* content analysis of MySpace. J. Adolesc. 2008, 31, 125-146.
45. Kallinikos, J. *The Consequences of Information. Institutional Implications of Technological Change*; Edward Elgar: Cheltenham, UK, and Northampton, MA, USA, 2006.
46. Nissenbaum, H. Will Security Enhance Trust Online, or Supplant It? In *Trust and Distrust Within Organizations: Emerging Perspectives, Enduring Questions*; Kramer, R., Cook, K., Eds.; Russel Sage Publications: New York, NY, USA, 2004; pp. 155-188.
47. Christofides, E.; Muise, A.; Desmarais, S. Information disclosure and control on facebook: Are they two sides of the same coin or two different processes? *Cyberpsychol. Behav.* **2009**, *12*, 341-345.
48. Tufecky, Z. Can you see me now? Audience and disclosure regulation in online social networks sites. *Bull. Sci. Technol. Soc.* **2008**, *28*, 20-32.
49. Debatin, B.; Lovejoy, J.P.; Horn, A.K.; Hughes, B.N. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *J. Comput. Mediat. Commun.* **2009**, *15*, 83-108.
50. Valkenburg, P.M.; Peter, J. The Effect of instant messaging on the quality of adolescents' existing friendships: A longitudinal study. *J. Commun.* **2009**, *59*, 79-97.
51. Solove, D.J. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*; Yale University Press: New Haven, CT, USA, 2007.
52. Ciocchetti, C. E-Commerce and information privacy: Privacy policies as personal information protectors. *Am. Bus. Law J.* **2007**, *44*, 55-126.

53. Palfrey, J.; Gasser, U. *Born Digital: Understanding the First Generation of Digital Natives*; Basic Books: New York, NY, USA, 2008.
54. Barnes, S. A privacy paradox: Social networking in the United States. *First Monday* **2006**, *11*, Available online: http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394 (accessed on 3 August 2011).
55. Herring, S.C. Questioning the Generational Divide: Technological Exoticism and Adult Construction of Online Youth Identity. In *Youth, Identity and Digital Media*; Buckingham, D., Ed.; MIT Press: Cambridge, MA, USA, 2007; pp. 71-94.
56. Spanbauer, S. Safeguard your reputation while socially networking. *PC World* **2006**, *24*, 152-154.
57. Haidt, J. The emotional dog and its rational tail: A social intuitionist approach to moral judgment. *Psychol. Rev.* **2001**, *108*, 814-834.
58. Nissenbaum, H. Privacy as contextual integrity. *Wash. Law Rev.* **2004**, *79*, 119-158.
59. Floridi, L. The ontological interpretation of informational privacy. *Ethics Inf. Technol.* **2005**, *7*, 185-200.
60. Palfrey, J. The public and the private at the United States border with cyberspace. *Miss. Law J.* **2008**, *78*, 241-294.
61. Youn, S. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *J. Consum. Aff.* **2009**, *43*, 389-418.
62. Moor, J. What is Computer Ethics? In *Computers & Ethics*; Ward-Bynum, T., Ed.; Blackwell Publisher: Malden, MA, USA, 1985; pp. 266-275.