European Citizens and Their Trust in Social Networks

Gianmarco Baldini[1], Ioannis Kounelis[1,2], Jan Löschner[1], and Mariachiara Tallacchini[1]

[1] Institute for the Protection and Security of the Citizen
Joint Research Centre (JRC), European Commission, Ispra (VA), Italy
[2] Royal Institute of Technology (KTH), Stockholm, Sweden
{gianmarco.baldini,ioannis.kounelis,jan.loeschner,
mariachiara.tallacchini}@jrc.ec.europa.eu

Abstract. In information and communication technology (ICT) trust has been considered as a crucial component of digital interactions. Trust has been dissected in a variety of potential meanings and dimensions and through the merging of trust in humans and trust in machines. In this paper, we investigate the role and the aggregation of trust in social networks and blogs and how it relates to knowledge production, and its connections to concepts such as reputation and sustainability in the European context. Moreover, we discuss knowledge production in information and communication technology and its relationship to user trust. We develop a view on the co-production of knowledge and trust and propose a policy management framework to support the users in their trusted use of social networks and blogs. This is presented based on an e-health use case analysis considering web based reputation and developing a new reputation scheme.

Keywords: trust, social networks, European citizens, collaboration, reputation, e-health.

1 Introduction

The relations between trust and modes of knowledge production have been widely explored by scholarly work in sociology of science, where they have been shown as an essential part of the renewal of the social contract between science and society [1, 2]. On the one hand, the involvement of lay citizens in the making of science and the concept of peer-production of knowledge between experts and non-experts are envisaged today as strategic ingredients to improve scientific and technological learning processes and make them more robust and trusted. On the other hand, trust is increasingly needed in all relationships –be they related to knowledge, personal, professional, and social life.

In information and communication technology (ICT) trust has been considered as a crucial component of digital interactions, and has been dissected in a variety of potential meanings and dimensions –and through the merging of trust in humans and trust in machines. Trust and confidence have different shades of meanings. However, here we propose to define trust as the level of confidence, which an entity can ensure

P. Zaphiris and A. Ioannou (Eds.): LCT 2014, Part II, LNCS 8524, pp. 363–374, 2014.

to another entity or entities for specific services and in given context [3]. Even if trust has been often used with reference to human beings, trust can also be associated to a machine or digital system (e.g., web site), which points out the importance of analysing and measuring the level of trust in a digital society.

In ICT knowledge production has entered the debate as a possible path to trust as it represents a vehicle for valued and respected relationships. Collaboration in knowledge processes has been at the core of the most traditional scientific community ethics –namely the so-called "ethos" of science. Today, knowledge co-production can contribute to trusted ICT digital interactions [4, 5]. European citizens' values and fundamental rights provide a specific framework that needs to be explored, together with its opportunities and challenges.

In this paper, we investigate the role of trust in social networking services and how it relates to knowledge production, and its connections to concepts such as reputation and sustainability in the European context. In comparison to conventional social networks, there are important differences to be considered:

1. The persistence of information about individuals, which impacts the personal sphere in particular its privacy or security,
2. The possibility to provide real-time updates on the life of the individuals thanks to the pervasiveness of the internet and wireless communication,
3. The possibility of masquerading behind a web page, which can become both a protection of the individual and a liability if used by malicious entities.

We expand in this paper the concept of social networking services to include other forms of citizens' interactions through digital technologies (e.g., blogs). In continuously changing digital ecosystems, where new technologies appear in the wider context of the internet and have an impact on the ethical sphere of the citizen (e.g., wearable sensors, e-health), it is very important to define a model for trust providing a measurable level of confidence and trust to the citizen as user. This trust model must be technology agnostic to address the future evolution and it must be flexible enough to support different contexts or different regulations/policies defined at national or European level. In particular, we will investigate potential future extensions of social network services regarding mobility, wearable sensors (e.g., including medical devices) and the increasing role of eGovernment services. This paper also reviews the existing models of trust in literature (e.g. reputation or credential based, institutional) and their applicability to social network services.

On the basis of the previous considerations a new model of trust based on a policy management approaches is proposed and described. This model is applied qualitatively to the scenario of social networking services and blogs related to the domain of e-health, where entities (e.g., research centres, e-commerce sites) from different domains with different levels of reputation can provide information and services. On the one hand, this is an area where citizens are increasingly looking for information and knowledge to improve awareness and make informed decisions regarding their personal health. On the other hand, considering the wide range of offers (both in terms of information and products) available on the web, there is an increased risk that the provided information could be dangerous or incorrect. The potential consequence of an absence of trust indicators in these sites is that the citizen can be exposed to considerable risks both for personal information (i.e., privacy), and for his/her health and safety, as incorrect or inappropriate information and products can be harmful rather than beneficial. Finally, the paper also links the provision of trust in this domain to supporting more sustainable and safe ecosystems as indicated in [6].

This contribution is structured as follows. The next section introduces knowledge production in information and communication technology and its relationship to user trust. In section 3 we introduce a policy management framework. In section 4 we discuss mechanisms to support reputation in the Web, and in section 5 we illustrate the discussion with some online examples. In section 6 we present an e-health use case and the analysis of a new reputation scheme. Finally, we provide some conclusions and an outline of our future work.

2 Co-production of Knowledge and Trust

The relations between modes of knowledge production and ethical behaviour have been at the core of the intertwined foundations of the validity and ethical soundness of science as well as of the trustworthiness of the scientific community. Indeed, the most traditional framing of the so-called ‘ethos’ of science — as portrayed, for instance, by Robert Merton [17]—interprets scientific practices as simultaneously generating and replicating sound knowledge and moral conducts, in a co-production of epistemic and normative dimensions [16]. As known, four main characters compose the ‘ethos’ of scientific knowledge as a certified stock of knowledge and a set of cultural values: universalism, communism, disinterestedness, organized scepticism. Universalism refers both to the universal character of scientific knowledge and to its not being bound nationalities or cultures; communalism entails that scientific results are the common property of the entire scientific community; disinterestedness assumes that common good and not personal gain is the purpose of the scientific endeavour; organized scepticism means that scientific claims must be exposed to the peers’ critical scrutiny before being accepted.

Altogether, these elements were deemed reliable in constituting and legitimizing the scientific community as a polity composed by ‘peers.’ In fact, at the same time these criteria refer to the knowledge practices embodied in scientific work and to the values that, while informing and guiding scientists’ conducts, consolidate and reproduce science as a cognitively and morally trusted social system.

After the neo-positivist vision of science as neutrally objective has been mostly abandoned, reference to scientists’ trustworthiness, namely their moral credibility, has become an integral part of the validity of science, both internally (within the community of experts) and externally (in the relations with society). In the redefinition of the relations amongst scientists, institutions, and the public, the rebuilding of trust has turned out as critical to the renewal of the social contract between science and society, in the face of scientific failures in preventing unforeseen consequences of new technologies —e.g. in the health and food sectors in the EU. A lack of trust was at the base of what EU institutions have called citizens’ ‘unease’ with science, namely their hesitant and unconfident behaviour towards technological innovation. Moreover, due to both the widespread dissemination of knowledge and the availability of technologies, scientific knowledge started happening in diverse social environments other than universities, academies, research centres [1, 2].

In the last two decades, ICT have increasingly and capillary encouraged a different mode of knowledge, relying on the spontaneous and collaborative creation and sharing of knowledge by scientists and lay people, experts and non-experts, meeting through the web in virtual communities and social networks. This co-produced, or crowd sourced, knowledge reveals a special value when it is shaped as 'commons-based peer production' of knowledge, namely when all parties involved are recognized as peers within the community [4, 5]. From this perspective, it is important to specify that, while 'crowd sourced' knowledge merely refers to a project soliciting participants' contributions, 'peer production' implies the genuine and as freely as possible sharing of those contributions amongst all participants [15].

This extended community of peers shows relevant similarities with the traditional scientific community in the mutual interconnectedness of its epistemic and moral foundations. As Benkler and Nissembaum have pointed out [4], *"socio-technical systems of commons-based peer production offer not only a remarkable medium of production for various kinds of information goods but serve as a context for positive character formation."* In fact, *"the emergence of peer production offers an opportunity for more people to engage in practices that permit them to exhibit and experience virtuous behavior".*

As known, the traditional ethos of science has revealed its limitations and rhetoric when, from ideal set of relevant epistemic and ethical criteria, it has become a self-referential and black-boxed way to establish validity and legitimacy —e.g. in science-based policy models, where political decisions claim to be neutrally based in scientific facts [18, 19]. In a similar way, peer production of knowledge needs to adopt deeper justifications towards the dynamically quest for trustworthiness.

In fact, if, on the one hand, the equal involvement of experts and lay people in knowledge-making as peers has become an essential ingredient in improving the scientific and technological learning processes and in making them more robust, transparent, and trusted; on the other hand, these overall processes have to constantly sharpening and deepening their search for trust through both technical and non-technical, human-based, criteria.

This unending search towards trust, namely trust as a process rather than a product, has a special meaning within the EU and for its citizens. Not only trust has been a critical element in the relations between the EU institutions and European citizens, but it is also an essential part of the European vision of rights and science policy [24].

3 Trust and Reputation in Regulatory Frameworks

In the European Commission, the concept of Trust belongs to one of the pillars of the Digital Agenda: the Third Pillar of Trust and Security [7], which is the basis for various actions of the Digital Agenda, including Action 28: Reinforced Network and Information Security Policy, Action 35: Guidance on implementation of Telecoms rules on privacy and Action 37: Foster self-regulation in the use of online services. This pillar is related to Data Protection Directive (namely Directive 95/46/EC) [8], which regulates the processing of personal data within the European Union. This directive is currently ongoing a review and a new regulation will supersede the existing provisions. Beyond the specific concept of privacy and data protection, trust services have been proposed as part of the recent regulation on electronic identification and trust services for electronic transactions in the internal market [10]. In the wider context described in this paper, there is a clear need to establish new guidelines or a regulatory framework to evaluate the level of trust in web services. A step in this direction is the definition of Privacy Seals [11], namely the development of *"an EU website labelling system, modelled on the European Privacy Seal, certifying a site's compliance with data protection laws (…) that (…) should include a thorough impact assessment and must avoid duplication of existing labelling systems"*. Public and private seals have been already developed in some European countries such as Germany, where the e-Ten project developed EuroPriSe4. In a similar way, the French Data Protection Authority is developing privacy seals for trainings and audits. In the USA, privacy seals are provided by private companies like TRUSTe [12]. However, despite these efforts, privacy seals may not be enough to guarantee that a user can fully trust a web service and its contents.

In the USA, the National Strategy for Trusted Identities in Cyberspace [9] highlighted the need to increase the level of trust of internet services towards the user. The main proposed approach, called Identity Ecosystem, is based on identification of the individuals and entities operating in the cyberspace in a way that can protect their privacy. Some of the main elements of the Identity Ecosystem described in [9] are:

- The subject of a transaction: a generic citizen or an application
- An identity provider, which is for establishing, maintaining, and securing the digital identity within the Identity Ecosystem.
- An attribute provider is responsible for the processes associated with establishing and maintaining identity attributes. Note that a subset of the real identity can be used or a new identity can be created for a specific context.
- An accreditation authority assesses and validates identity providers, attribute providers, relying parties, and identity media, ensuring that they all adhere to an agreed-upon trust framework.

Note that the Identity Ecosystem foresees the application of policies and standards even if a clear description of the related technical solutions is not included [9]. The Identity Ecosystem does also support change of the context or different roles, with different levels of access, so that specific roles (e.g., a doctor) can have access to personal data when there is a crisis or similar change of context from a “normal” situation. These features are also present in the framework we describe in this paper.

Communication with peers in the light of a cross border situation with different legal frameworks and possibly natural language barriers challenge even more the reputation mechanisms.

4 Mechanisms to Support Reputation in the Web

In [13], the authors describe various signal processing techniques, which can be used to support the security of reputation systems on the web: bayesian reputation systems where the reputation scores of a web entity can be updated on the basis of observations; belief theory based on probability; fuzzy logic and others. In [13] the most probable attacks to reputation mechanisms and related countermeasures are also identified.

One of the main drivers for attacks to reputation is the economic gain. For example, e-commerce web sites are increasingly based on reputation mechanisms to give an estimate of the reputation of a seller or a buyer. The feedback mechanism in eBay is well known, but also other web sites use a review-based approach where customers of an online or physical (e.g., restaurant) merchant can provide a review on the received service. On the basis of the positive or negative reviews, a host application or web service can create a sorted reputation list of the merchants. This review mechanism does not exist at the moment for all the online services. The healthcare information sites described in the introduction may also benefit from a simple feed-back/review mechanism but, as described in [14], there are various techniques to at-tack such a simple mechanism and undermine the overall reputation framework. For example, malicious users can generate fake feedbacks by creating a large number of pseudonyms in reputation frameworks where the feedback is linked to an identity. Instead, in reputation frameworks based on reviews where the identity is not strongly enforced, professional paid writers can generate any type of positive or negative review. The overall impact of these coordinated and even profit-driven manipulations can be a significant distortion of the reputation scores and a degradation of the overall reputation framework, which eventually undermine the level of confidence of the users.

Other popular reputation frameworks, which have been proposed for the online world, are based on the evolution of old-fashion approaches. One approach could be based on the collection of evidence from organizations, which have the objective or the professional capacity to provide impartial (or at least non intentional partial) feedbacks, which can be used to build trust. One example is a consumer organization. Another approach could be based on the opinion of experts, which are also supposed to be impartial. The model of the movie or restaurant critics can be reapplied to the online world. Both approaches have some strong disadvantages. In fact, their provided evidence is costly to collect and can become outdated very quickly with the evolution of web services; moreover, the large number of online web services requires, in order to be validated, a large number of experts in different fields. Under such circumstances it is difficult to build a proper business case and to support the reputation framework in a consistent way.

There is the need to define new models of reputation, involving both technical and non-technical criteria, which can overcome the limitations described before.

5 Online Examples

In our days a continuous growing number of often concurrent online services are dealing to gain clients. The business case is based on increasing membership numbers assuring a profitable service. An example already mentioned in this paper is eBay. The use case is becoming more sensitive in respect to security and data protection when the trust level concerns the user directly, for example in respect to his personal health. The historical "reputation framework" is the relationship between the medical doctor and his patients. Already in 2000 the EU founded in the framework of its Action Plan for Internet User Security the certification and rating of Trustworthy and Assessed Health Information on the Net. A digital trust mark for health information was proposed to assist users in assessing the trustworthiness of medical offerings on the Internet and to make the glut of information on the World Wide Web more transparent. Currently, the patients once getting sick stress social networks and seek for peers to get advice, decide treatments and self-medicate. An example is [22], which focuses its efforts: "*on offering readers and visitors to our site objective, trustworthy, and accurate health information, guided by the principles of responsible journalism and publishing. Our editorial philosophy is to use relevant and accurate content to promote a healthy lifestyle and facilitate disease prevention, as well as to offer clinically significant, medically reviewed information for those who are seeking answers to their health questions.*"

Web services such as online pharmacies use labels such as the "Trusted Shop Guarantee" [20] to proof the quality of service in respect to the security of transactions. The label itself uses trust marks and customer reviews as ranking criteria. The pharmacy actively encourages its clients to recommend the service in social networks such as Facebook [21]. In a number of cases the rankings published by the service providers only refer to the part of the service such as the timeliness of the delivery, but not to the level of knowledge in respect to the health problem.

6 Proposed Reputation Model

The reputation model proposed in this paper is based on the following elements:

- An authentication and authorization mechanism to ensure that only authenticated and authorized entities can contribute to the content of a social networks site.
- A policy management framework, where policies are defined to mitigate some of the limitations of reputation schemes that are described in section 3.

6.1 The Generic Policy Management Framework

The main objective of a policy management framework is to support the definition and application of policies in an ICT system. A policy defines the type of actions which can be executed in a specific context, what should be executed, who is allowed to execute these actions and under which condition. Policy management frameworks are usually based on an Event-Condition-Action (ECA) enforcement rule. In other words, an ICT system or a component of an ICT system receives an *event*, which requests a specific *action*. This *action* can be executed only if a *condition* (or more than one condition) applies. Usually the policy management framework provides two distinct functions: a) the policy reasoning which implements the logic to decide if an action should be performed and b) the policy enforcement, which actually enforces the rule. The policy reasoning process can be implemented through an extraction of a possible solution by composition or decomposition of pre-defined policies. This can be defined as the policy database. These two functions are usually implemented in two elements of the policy management framework: the Policy Decision Point (PDP) also called the Policy Engine because it implements the reasoning function and the Policy Enforcement Point (PEP).

The ECA rule is activated when an element of the ICT system (for example a node in a social networking site) receives an event, which triggers a chain of operations. The event includes information related to the original requester of the event, the type of service requested, the assets and resources on which the service must operate and so on. For example, an event can simply be the request of read access to a record. The event is processed by the PEP component in the node. This processing may include the extraction of the relevant information (type of service, source of the requester, as on which service must operate). Once processed, the PEP executes a policy query to the PDP, which can be hosted by another ICT system in the social networking sites. It is important that the communication between the PEP and the PDP is secure against eavesdropping, and that it ensures the integrity of the exchanged messages. The PDP examines the request and identifies the correct policy to adopt on the basis of the requested service and the *context*. With the word *context,* we mean the existing boundary conditions at the time the request has been received. These boundary conditions could be the number of other users already authenticated in the system, the specific condition of the social networking site (under maintenance), which may prevent the execution of the service request and so on.

On the basis of the content of the service request and the context, the Policy Reasoner in the PDP chooses the specific policy in the space of the policy database. The PDP then replies to the PEP with the policy itself. The PEP enforces the policy in the node. The PDP and PEP relationship is described in Figure 1.

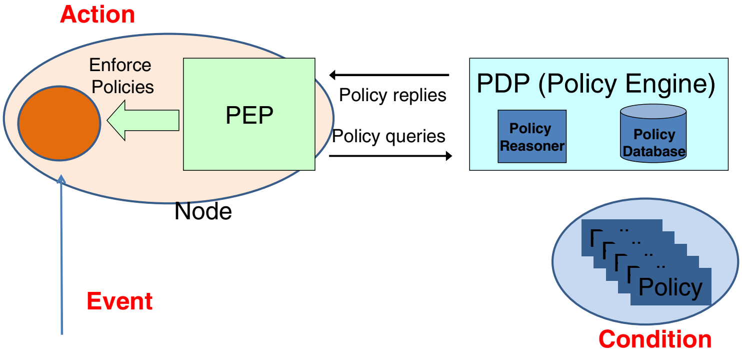

Fig. 1. Policy Management Framework

6.2 The Use of the Policy Management Framework in Social Networks

As we described before, the policy management framework must be combined with an authentication and authorization mechanism to ensure that only authenticated entities can insert content in the social network site. Any authentication technology can be used (e.g., sign-on, credentials). In the authorization phase, the authentication entity is associated to a specific role and type entity. In the example of the social networking site for medical equipment and medicines, the authenticated entity can be a doctor, a researcher, the representative of a consumer association or the representative of a product manufacturer or just a generic citizen. In all these cases, it is important to embed in the system the role of the authenticating entity. While some roles can provide information, which is supposed to be impartial (e.g., a doctor or researcher), in some other cases the provided information can be quite detailed but not impartial, due to a business interest (e.g., the representative of the product manufacturer).

The role of the entity is used in the PDP to understand the particular policy to be applied. For example, a social networking site can have a feedback/comments section, which provides reviews of a specific product. If a potentially partial entity (e.g., the representative of the product manufacturer) would like to provide a comment to the reviews section, the PDP can intercept this request and deny the provision of the content. This approach can be applied to any section of the social network site, so that only appropriate comments are posted in specific areas. In another example, the PDP can check the number of entities, which provided past reviews, and deny a new contribution if an entity has already provided too many reviews to increase the positive or negative feedback on a product.

The policy framework can also be used to implement intelligence in the social networking site to improve the overall robustness of the web site against security/privacy attacks. For example, they can intercept a security or privacy attack by denying a service request, which tries to have access to many instances of personal records of the social networking site. In this context, policies can be used not only to deny or allow data breaches but also to emit notifications to the administrators of the social networking site in case of suspicious behavior of entities during authentication.

New policies can be created at any time in response to a change in the context to address the misbehavior of an entity, which can be a contributor or a product manufacturer. For example, if the administrator of a website receives a notification that there is a suspect medical product in the market, a policy can be immediately implemented to deny procurement of this medical product by users.

The adoption of a policy management approach can be used to mitigate the challenges presented in section 3 in the following ways:

1. *Fake feedbacks in the review mechanism.* In this threat to the reputation mechanism of the social networks, fake feedbacks are generated to alter the review rate of a specific product or evaluation of a cure. This threat can be mitigated through the definition of policies, which can be triggered to analyze patterns or anomalies in the provided feedback. Two examples are identified: in the first example, specific patterns or commonalities can be identified and analyzed like similar feedbacks or feedbacks originating from users with the same IP address or the same location. In the second example, when an entity is applying for a new feedback review, the policy can request a "similarity" check on all the existing feedback/reviews against the opinion of the experts. Note that the policy management approach can also be applied in the authentication/authorization phase to detect the generation of a large number of pseudonyms. While some information can be faked (name, surname), a check can be done against the originating IP address or the provided physical address to detect anomalies. This check can be

implemented in the policy itself. In this way, we can prevent the generation of a large number of pseudonyms.

2. *Reputation frameworks based on reviews where the identity is not strongly enforced*. In this threat, entities can provide contributions but there is no link to the identity of the entity or its role. In the proposed framework, this threat is mitigated by the authentication and authorization mechanism, where the entity's identity and role are recorded and used in the policy management framework. In addition, policies can be used to highlight the content provided by the entities and their level of reputation in the social networks. This will give an immediate indication to the user of the social networks on how much the contribution can be trusted.
3. *Evaluation of the trust of the presented content*. The policy framework can implement additional checks on the validity of the information provided. To achieve a substantial level of trust, the provided content must be supported by scientific studies. The policies can implement a check on the presence of scientific studies on a specific medical cure or the results from scientific trials on a medicine.
4. *Natural language barriers of users.* The policy framework can define a policy agnostic to the natural language to support interoperability within a domain in a cross border environment.

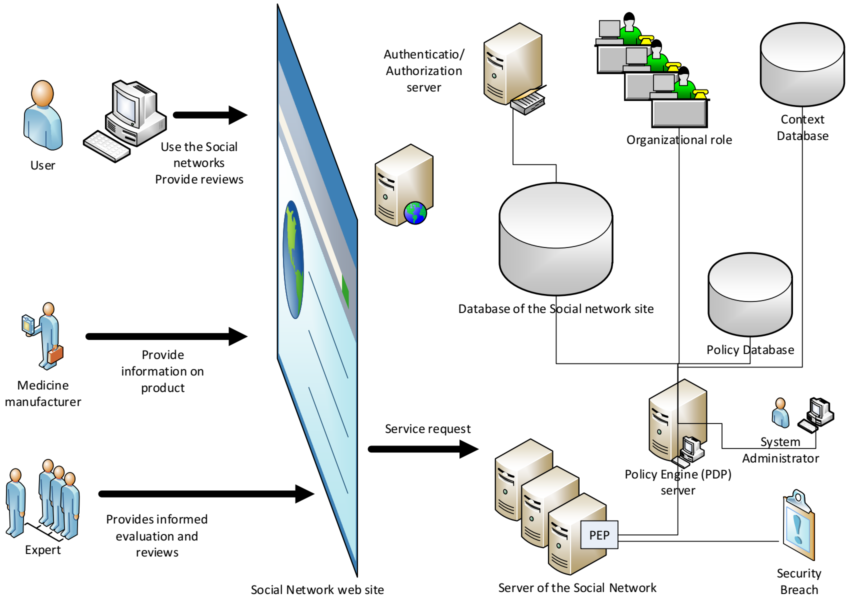
User
Use the Social networks Provide reviews
Medicine manufacturer
Provide information on product
Expert
Provides informed evaluation and reviews
Social Network web site
Authenticatio/ Authorization server
Organizational role
Context Database
Database of the Social network site
Policy Database
Service request
Policy Engine (PDP) server
System Administrator
PEP
Server of the Social Network
Security Breach

Fig. 2. Policy Framework for a Social networking site

The overall elements of the proposed framework are shown in Figure 2. The PEP components must be implemented and deployed in the main servers of the social networking site, while the policy engine/PDP function can be implemented and hosted in a specific server, which has access to various sources of information in the system, including the database of the social networking site, the policy database and the context database. The Authentication/Authorization server takes care of authenticating the user and matches their identity to a predefined organizational role. As described before, the policies can also be used to mitigate security threats and to notify the system administrators.

7 Conclusions

The evolution of the Web services and applications can support new ways of knowledge production, where both experts and lay people can participate as peers. One example of this evolution is the social network, which can support the collaboration in the knowledge processes, which has been at the core of the most traditional scientific community ethics –namely the so-called "ethos" of science. An essential element for an effective knowledge production is trust among the entities, which collaborate through the social networks.

The idea that valid knowledge and ethical behavior should generate each other in the scientific community, as traditionally portrayed in sociology of science, has re-emerged in relation to the specific features of peer-production of knowledge made possible by the web and ICT. However, here reliability of both knowledge and human behaviour require that trust is constantly renewed through a continuous process involving technical and non-technical criteria. In other terms, the knowledge process should encompass also the knowledge and commitment towards the adoption of shared reliable policy agreements and mechanisms. Support for trusted collaboration can be quite challenging both at an organization and technical level and this paper has highlighted some of the most significant challenges in this area. It remains difficult to build successful business cases and to support in a consistent way the reputation framework.

Future developments will explore more in detail how more advanced forms of the policy management framework, such as presented in [23], can support more effective knowledge production and trusted collaboration in social networks.

References

1. Gibbons, M., et al.: The new production of knowledge: the dynamics of science and research in contemporary societies. Sage, London (1994)
2. Nowotny, H., Scott, P., Gibbons, M.: Rethinking science: knowledge in an age of uncertainty. Polity, Cambridge (2001)
3. Ion, M., Danzi, A., Koshutanski, H., Telesca, L.: A peer-to-peer multidimensional trust model for digital ecosystems. In: 2nd IEEE International Conference on Digital Ecosystems and Technologies, pp. 461–469 (2008)
4. Benkler, Y., Nissenbaum, H.: Commons-based Peer Production and Virtue. The Journal of Political Philosophy 14(4), 394–419 (2006)
5. Benkler, Y.: The Penguin and the Leviathan. Random House, New York (2011)
6. Jin-Hee, C., Chan, K.S.: Building Trust-Based Sustainable Networks. IEEE Technology and Society Magazine 32(2), 32–38 (2013)

7. European Commission: Digital Agenda for Europe. COM, 245 (2010), http://ec.europa.eu/digital-agenda/ (accessed December 17, 2013)
8. European Parliament and Council: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281/31 (1995)
9. The White House: National Strategy for Trusted Identities in Cyberspace (2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (accessed January 15, 2014)
10. European Parliament and Council: Regulation of The European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. COM/2012/0238 (2012)
11. European Parliament: European Parliament resolution of 15 December 2010 on the impact of advertising on consumer behavior. Official Journal of the European Union, C 169 E/58 (2012)
12. Truste, http://www.truste.com (accessed February 7, 2014)
13. Yan, S.: Security of Online Reputation Systems: The evolution of attacks and defenses. IEEE Signal Processing Magazine (29), 87–97 (2012)
14. Yang, Y., Feng, Q., Sun, Y.: Dai.Y.: Reputation trap: An powerful attack on reputation system of file sharing p2p environment. In: 4th Int. Conf. Security and Privacy in Communication Networks (SecureComm 2008), Istanbul, Turkey (2008)
15. Ball, M.: 23andme's First Patent (2012), http://madprime.org/articles/2012/05/23andmes-first-patent (accessed January 30, 2014)
16. Jasanoff, S.: States of Knowledge: The Co-production of Science and Social Order. Routledge, New York (2004)
17. Merton, R.K.: Science and Democratic Social Structure. In: Social Theory and Social Structure, pp. 604–615. Free Press, New York (1968)
18. Tallacchini, M.: Between uncertainty and responsibility: precaution and the complex journey toward reflexive innovation. In: Vos, E., van Asselt, M., Everson, M. (eds.) Trade, Health and the Environment: The European Union Put to the Test, pp. 74–88. Routledge, London (2014)
19. Wynne, B., et al.: Taking European Knowledge Society Seriously. European Commission, EUR 22700 (2007)
20. Trusted Shops, http://www.trustedshops.eu/ (accessed February 7, 2014)
21. Facebook, VfG Versandapotheke Österreich, https://www.facebook.com/VfG.Apotheke.at (accessed February 5, 2014)
22. Healthline, http://www.healthline.com/health/about-healthline (accessed January 15, 2014)
23. Neisse, R., Doerr, J.: Model-based Specification and Refinement of Usage Control Policies. In: Eleventh International Conference on Privacy, Security and Trust (PST), Tarragona, Spain (2013)
24. Funtowicz, S., Strand, R.: Models of Science and Policy. In: Traavik, T., Lim, L.C. (eds.) Biosafety First: Holistic Approaches to Risk and Uncertainty in Genetic Engineering and Genetically Modified Organisms, pp. 263–278 (2007)