Privacy-by-Norms
Privacy Expectations in Online Interactions

Theodore Patkos*, Giorgos Flouris*, Panagiotis Papadakos*, Antonis Bikakis†, Pompeu Casanovas‡,
Jorge González-Conejero‡, Rebeca Varela Figueroa‡, Anthony Hunter§, Guðjón Idir††, George Ioannidis¶,
Marta Kacprzyk-Murawska‖, Andrzej Nowak‖, Jeremy Pitt**, Dimitris Plexousakis*,
Agnieszka Rychwalska‖ and Alexandru Stan¶
*Institute of Computer Science, Foundation for Research and Technology - Hellas
†Department of Information Studies, University College London
‡Political Science and Public Law Dept., UAB Institute of Law and Technology
§Department of Computer Science, University College London
¶IN2 Search Interfaces Development Ltd
‖Institute for Social Studies, University of Warsaw
**Electrical and Electronic Engineering, Imperial College London
††IMMI International Modern Media Institute

***Abstract*—In an increasingly instrumented and inter-connected digital world, citizens generate vast amounts of data, much of it personal, and nearly all of it valuable. However, controlling who can collect it, limiting what they can do with it, and determining how best to protect it, remain deeply undecided issues. This position paper proposes a socio-technical solution based on collective awareness and informed consent, whereby data collection and data protection norms are configured by the users themselves, using a collaborative participatory process of argumentation. This refers to the ability of users to understand privacy-related documents and their implications via participatory processes, wisdom-of-the-crowds approaches and visual cues. By strengthening the trust bond between service developers and users, the transformative impact of this solution, called Privacy-by-Norms (P_bNorms), will be to encourage innovation and to ensure that (big) data's (tiny) generators are also its beneficiaries. P_bNorms will aim to complement existing top-down solutions to data protection that rely on technical or legal provisions. The goal is to enable citizens to express their privacy expectations through the use of mature ICT technologies from the fields of Computational Argumentation and the Semantic Web.**

I. Introduction

The seemingly relentless march of Moore's Law has arguably led to the realisation of Weiser's vision [1] of ubiquitous computing and the Internet of Things. The dramatic progress brought about by Information and Communication Technology (ICT) and at the same time its vast infiltration in almost all aspects of daily life has left society bemused over certain important issues, such as privacy management. The use of surveillance cameras on unmanned aircraft systems seems to produce a visceral hostile reaction from citizens who seem otherwise passively tolerant of fixed CCTV. Similarly, we will carry any number of objects with embedded sensors generating streams of data without objection, but will be suspicious of, or implacably opposed to implant devices – the only difference being whether the sensor is on or under the skin.

Lacking a broad understanding of the potency of digital services, we often adopt some surprising, and sometimes contradictory, attitudes. We want the benefits of personalised digital services, but also expect our private data to remain private. Privacy preservation is essential in human relations, democracy, independence and reputation, yet we frequently give our consent to untrustworthy software to collect, store and process our data, having limited evidence as to how this information will be protected or who has access to it.

Anonymity in the digital world has become all the more difficult to protect and this is more clearly pronounced in the world of smartphones and personal mobile devices. These devices encapsulate all those features that justify their frequent characterisation as ideal advertising platforms or tracking devices: they store information about our location, identity, friends, even our passwords, and they can easily be used to extract behavioural patterns, preferences and daily routines.

Relevant regulations exist, most notably in Europe, where the so-called General Data Protection Reform (GDPR) will soon be enacted, relying on principles like privacy-by-design, liability, transparency and data minimisation. Yet, the astonishing speed with which ICT progresses has deprived policy makers of the control over the procedures that can rapidly adapt to new technological developments; when it comes to digital technologies, legislation is usually a few steps behind.

Here, we advocate the need for social, collective *norms* to foster user empowerment towards privacy. To protect privacy adequately, society needs awareness, but also consensus on protecting measures and processes that generate social norms, with which service providers will voluntarily comply because it is profit maximising [2]. Towards this, we propose the Privacy-by-Norms (P_bNorms) paradigm, aiming at strengthening the bond between digital service providers and users. We describe how ICT tools can be coupled with the collective power of people to generate norms that can have sustainable impact on society and improve citizen awareness, through a collaborative participation process for reaching consensus between users and stakeholders. A knowledge commons ap-

proach to privacy policy is suggested, relying on bottom-up generated content and ICT solutions that can complement top-down legislation or technical privacy protection measures.

The rest of the paper is structured as follows. Section II sets the current privacy landscape related to digital services. Section III describes the main notions of the P_bNorms paradigm, while Section IV proposes ICT solutions to implement P_bNorms. Section V discusses strategies to approach users and stakeholders, while Section VI concludes the paper.

II. Data Protection

According to the European Commission[1] (EC), 72% of European citizens use the Internet at least weekly. In 2011, an average of 93% Europeans aged 16-24 used the Internet on a daily basis and 60% of children aged 9-16 access the Internet (almost) daily [3]. Moreover, the number of smartphone users in Europe and worldwide is growing with an increasing rate: by 2016, smartphone users globally will be more than 2 billion, and it is expected that over half of mobile phone users will operate smartphones in 2018.[2]

A Eurobarometer expressly dedicated to the public perception of online privacy and data protection[3] showed that, in 2011, European Internet users had already given out voluntarily their real name (79%), personal photos (51%), actual home addresses (39%), phone numbers (23%), and personal identity documents or IDs (13%). At the same time, the EC[4] emphasised that "58% of Internet users read privacy statements online", even though "62% of users either do not understand, do not read, cannot find, or ignore such privacy statements", according to their own perception. The Green Paper on Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values, published by the EC in 2013[5], stressed that, in 2012, 22% of citizens in the European Union (EU) used a mobile device to access the Internet, underlying the necessity for improving quality content addressed to minors, as well as protecting minors when they go online.

The EU, being aware of this evolution, is trying to adapt its approach to personal data protection: in 2009, the existing regulation of personal data processing and privacy protection in electronic communications was reformed through Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009. This new Directive amended both Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector, and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. In 2012, further reform was proposed of what was the general legal framework on data protection. The GDPR package includes a general instrument and a concrete legal text on data use by police forces.

Although the efforts of the EU and its Member States in this field have been very fruitful, the enactment of regulations and directives has not been sufficient and users of online services still suffer from privacy violations and see their personal data misused. The structured nature of law and traditional regulatory mechanisms may sometimes be incompatible with or unsuitable for the swift changing nature of ICT technologies. Online services, moreover, operate on a global scale, while law is by definition limited to a geographical context. The EU has foreseen both the protection of personal data in the processing phase and the protection of individuals when such data are transferred. The problem still arises in those cases in which the transfer occurs outside the territory in which the EU and their Member States are competent. Furthermore, the existence of General Terms and Conditions (GTC) or end-user license agreement (EULA) documents, which include more detailed explanations in a legally formal manner, creates additional problems. Even though in order for GTC to be binding they have to fulfil some requirements -essentially, not to be abusive - the mere fact that they are written in a complex manner makes them only accessible to trained legal experts.

EU institutions have stressed that individuals must be empowered to be able to protect their rights. Citizen empowerment policies strongly rely on the provision of clear, accessible information. In this regard, ICT technologies have a strong potential to provide accurate information on key aspects for ICT platform users. Among these aspects, the ones related to privacy are of the utmost importance, as most users are not aware of the rights provided by European, national, and local laws. The provision of clear and up-to-date information is critical to empower users and enable more suitable choices before downloading/buying a software product.

III. Collective Norms for Privacy Expectations

Against the current landscape in the digital world, the protection of privacy is not just the result of applying legal and technical requirements. It seems to be also connected with the idea of the personal privacy expectations of each individual, an expectation that also depends strongly on the context in which the user is interacting (e.g., media sharing sites, social networks, apps). Digital awareness has become a key issue and, consequently, citizens are another link in the chain of protecting their own privacy. In this regard, the improvement of the individual's empowerment may be the missing link in the implementation of a comprehensive and effective global strategy for the protection of privacy in the digital age.

There are 3 critical technological innovations in P_bNorms:
1. Rule-based Knowledge Commons. Participatory sensing is the process of leveraging user devices (each of which is equipped with multiple sensors, for measuring location, health indicators, etc) to collect data from many sources, aggregate it, and analyse it to derive some information and/or knowledge. From the P_bNorms perspective, we construe the aggregation of data as a common-pool resource, which is provisioned to

[1]Digital Agenda Scoreboard 2014

[2]http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694

[3]Attitudes on Data Protection and Electronic Identity in the European Union - Special Eurobarometer survey 359, European Commission, 2011.

[4]Press Release: Data Protection: Europeans share data online, but privacy concerns remain - new survey. June 2011

[5]http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0231:FIN:EN:PDF

Fig. 1. P_bNorms visual cues.

by data generators, appropriated from by analysts who process the information to create new information and/or knowledge from the raw data, and benefited from by consumers, in the form of products or services derived from the knowledge.

However, in any participatory-sensing application the roles of *data generator*, *analyst* and *consumer* are not necessarily mutually exclusive; but they are often asymmetric. In particular, while the data generators run the risk of an invasion of their privacy, if potentially sensitive data is used in inappropriate ways, it is the analysts, acting as consumers, who will benefit mostly from the use of such data. In other words, the risk is socialized, but the profit is privatised.

To help overcome this issue, the first innovation of P_bNorms is, having construed participatory sensing in terms of a knowledge commons, to formally characterise that construal using computational logical rules to specify and enforce *appropriate* norms of behaviour, on the part of the different actors in the system with regards to data privacy and protection. Moreover, these rules allow the representation of the governance of the system and specifically its privacy policies as code, using computational logic.

2. Design Contractualism. Design contractualism is the idea that developers make legal, moral or ethical decisions and then (a) embed these decisions in the code itself and (b) make those decisions manifest to the user. Part (a) is achieved by encoding rules of order for appropriate behaviour in computational logic as above, so the second critical innovation is to make those rules manifest to the different actors in the system. Since we are dealing with a knowledge commons, one approach is to extend an idea from the creative commons.

For example, Creative Commons supports six different licences in three "layers", the Legal Code layer as understood by users, the Human Readable layer, a user-friendly interface to the legal code layer in a form that people can understand, and the Machine Readable layer, a summary of the key freedoms and obligations written into a format that software systems, search engines, and other kinds of technology can understand. For the Human Readable layer, this is indicated in iconic form, indicating for instance that a given license allows others to manipulate and build on a creative "work of mind", but requires crediting the creator, provided it is for non-commercial purposes, and such extended creations are distributed under the same terms. Essentially, each of these conditions is a norm, as it serves to coordinate expectations (but in this case the norm also has legal implications if the norm is violated). However, one can imagine a user group operating under one licence, but reaching a point where they would prefer to operate under a different licence: the question is how to agree changes in licensing arrangements.

In P_bNorms, we propose the use of similar iconic representations to link the data privacy and data protection rules. For example, the icon in Fig. 1 could indicate that an application endorses (or is endorsed by) P_bNorms, and observes the proportionality and time-of-use principles (data is only stored until it has been used for the purpose for which it was collected). Effectively, we want to do for privacy in knowledge commons what Creative Commons has done for works of mind: images, books, software, etc. However, P_bNorms also allows modifying the norms.

3. Collective Choice by Argumentation. The third critical innovation is collective choice: the system participants affected by the rules also participate in their selection and modification. The EU highly appreciates Collective Awareness Platforms (CAPs) as an instrument for social participation and innovation [4] and techniques from the field of Computational Argumentation have already found their way to such platforms.

Privacy protection and management, as well as information sensitivity, are inherently user-centred, thus it cannot be claimed that a given set of norms for a given app is suitable for all users and contexts. In the P_bNorms model, when the debate for norm generation starts, the members may have totally different perspectives and needs, therefore, as the debate progresses, it should identify groups of people sharing common opinions. Once this happens, a separate debate per group can specify the corresponding fit-for-purpose norms.

The identification of groups can be formally represented in the governance rules by the notion of empowerment and the formal characterisation of role. For any group, access-control procedures can be defined, which assign to specific individuals certain roles. With the notion of empowerment, these roles are associated with certain rights, such as, for example, enfranchisement, or the right to vote. This can be represented in terms of (institutionalised) powers and entitlements, for example, the power to cast a vote, and an entitlement to have it counted correctly, and for the outcome to be declared correctly.

These guidelines can be adapted to enhance the privacy policies of diverse digital services. Apps for mobile devices, for instance, specify the groups of capabilities or information (permission groups - PGs) that they need access to. Many platforms, such as Android, operate on a take-it-or-leave-it style, leaving a lot of aspects inadequately supported; in particular, developers are not required to explain why they need access to the requested PGs and what they plan to do with the respective data. P_bNorms will expand the current scheme with support for explanation generation and justification modelling: for each PG that some app requests access to, the justification can comprise a set of aspects denoting why the app developer needs this PG and a set of aspects denoting the user benefits. Our proposed solutions intend to facilitate discussion about the *privacy scope* of apps with regards to data access, and enable users become aware and understand how their data is manipulated, as well as to express their privacy expectations.

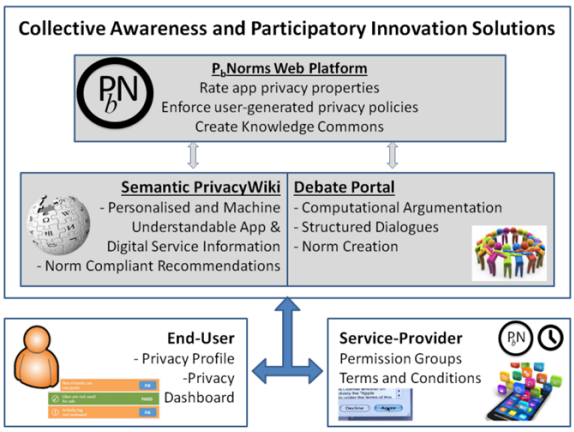

Fig. 2. Overview of main components.

This is closely related to the future plans of W3C[6].

IV. CAPs for Privacy Norm Generation

As our understanding of the dynamics of collective processes deepens, the coupling of CAPs with mature ICTs will manage to achieve more sustainable solutions. Decision-making processes and awareness platforms have much to gain if they embody technologies that can make them simpler, more credible, and more sensitive to the different personality attributes. In particular, we propose the use of technologies from the Semantic Web [5] and Computational Argumentation [6] fields as the main promoters of future CAPs, especially in the field of privacy awareness and policy making. In the sequel, we attempt to suggest solutions that can achieve a paradigm shift towards privacy-aware socio-technical components. Fig. 2 gives a schematic overview of such components.

Semantic Web technologies advocate the representation of information in a platform-independent, machine-interpretable and semantically-enriched format. This enables representing legal and technical information and terminology about norms, apps and Terms and Conditions documents in a language appropriate for the profile of each user, while at the same time being amenable to automated processing and reasoning. A Semantic Wiki is a direct application of these ideas into an effective awareness platform, as its utility widely relies on collaborative user behaviour and has already been adopted in various forms by other CAPs (e.g., Wikirate[7]).

The utility of a so called Semantic PrivacyWiki can rely on *feedback* provided by the crowd regarding how each request for access to a certain PG (e.g., GPS, contacts, camera etc.) by a given app is perceived, i.e., whether the user finds it reasonable. This can help build a (private) user profile in a non-intrusive way and allow personalised *recommendation services*, which will suggest applications that fit the user needs without violating her privacy in a manner that she would find unacceptable (according to her profile and/or norms she has associated herself with). Note that what one user considers an acceptable privacy violation (e.g., to get a free app, or to avoid advertisements), could be unacceptable for another.

The provided feedback will also be important for provoking interaction and discussion within the community about the expected or "reasonable" PGs that an app should require access to, according to its type and functionality. As there may be different viewpoints of the matter, this type of debating is crucial for proposing new privacy-related norms, or modifications of existing ones. This interaction can be facilitated by a *Debate Portal*, which will aggregate, organise and analyse opinions, thereby enabling users to engage in informed, well-defined and collective norm-developing processes.

Development of the Debate Portal can rely on theories, techniques and tools from the field of Computational Argumentation, which provides the theoretical background and the tools necessary to understand how conclusions can be reached through logical reasoning in the presence of possibly contradictory evidence for/against a certain conclusion [6]. This will enable formalising debates as sequences of inter-related arguments, whose analysis will provide the justifications necessary for users to reach an informed consensus on norms faster. Towards this aim, ontologies for representing arguments [7] and web-based tools for argument analysis and visualisation [8] will also be useful.

The P_bNorms approach, using a rule-based norm representation, its iconic visualisation, and the argumentation process for collective choice, engenders and enhances *collective awareness* of data privacy and data protection, because (a) the conditions on data usage are both accessible to the "human layer" and processable by the "machine layer", and (b) why the conditions on data usage are as they are is recorded (by the argumentation process). The P_bNorms approach is to treat big data as a "knowledge commons", i.e., a common-pool resource of data that can be provisioned to and appropriated from. However, we want this common-pool resource to be sustainable and resistant to free riding.

It had been theorised that all such common-pool resource would be subject to the tragedy of the commons, whereby a group of actors would act to deplete a common-pool resource in the short-term, even if it was in none of their interests in the long-term. However, political scientist and economist Elinor Ostrom demonstrated that throughout time and geography communities managed to avoid the tragedy by defining their own self-governing institutions, which she defined as sets of rules for managing resource [9]. Ostrom also observed that in all success stories of sustainable communities, the used rules had eight common features, which she re-phrased as institutional design principles.

A key aspect of P_bNorms is that it embodies some of those principles and therefore lays the foundation for sustainable knowledge commons. For example:

- Boundaries: the application members and the considered common-pool resources are clearly identified;
- Congruence: the provision and appropriation rules are, or

[6]System Applications Working Group meeting minutes: http://www.w3.org/2014/07/permissions

[7]http://wikirate.org/

can be made to be, congruent with the local conditions;
- Collective choice: those who are affected by the rules get to participate in their selection and modification.

V. Maximising Impact

Mechanisms for specifying the intended information use have been suggested in the past, e.g., the P3P protocol[8], but never achieved wide acceptance. The bottom-up participatory innovation paradigm of CAPs offers the means to achieve a more substantial impact, but society-wide participation and engagement are key aspects for its success. The most important difficulty that most "young" CAPs face is how to reach a critical size above which payoff for the platform (however defined) becomes positive. In order to overcome this *initial threshold effect* [10], a multi-dimensional strategy is needed to promote user engagement and foster social innovation.

A. Engaging Society in Developing Innovation

Norms are intrinsically social, so in order for social norms to emerge, the atomistic and self-centred individuals need to form groups. Turner [11] defines groups as "two or more individuals who share a common social identification of themselves or (...) perceive themselves to be members of the same social category". Sometimes, this collective perception of unity is the sole commonality that people within a social group share, but it nevertheless suffices to drive common action. Such awareness of group membership is most of the time latent, i.e., not consciously active, but in certain situations it becomes extremely salient and drives decision-making. As stated by Kellogg and Erickson [12], "collective awareness occurs when two or more people are aware of the same context and each is aware that the others are aware of it". In moments of activating collective awareness, all values, norms and social rules of the group are activated as well. Collective awareness thus underlies many social phenomena like peer pressure, accountability, collaboration and competition, and as such is a major driver of collective and individual action.

Any social innovation or sustainable social change relies on the creation of social systems that exhibit collective awareness and norms aligned towards specific, socially desired goals. Designing such systems is not a trivial thing even in real life situations. It becomes even harder when interaction happens online, where visibility and hence accountability is limited. On the other hand, ICT tools enable access and connection to an enormous number of potential members of the collective, which seems to increase the likelihood of finding enough motivated individuals to start and maintain a thriving community or organization. However, practice shows that only few communities manage to survive and grow and there is so far no recipe for effective online social systems and CAPs.

To facilitate the creation of CAPs, we need to capitalize on ICT-enabled possibilities and advantages. There is a difference between collectives gathered around popular items (like communities contributing remixes or localised versions of popular YouTube videos) and a thriving collective that has a potential to induce social change. What distinguishes CAPs like Wikipedia is the development of social norms, shared values, common goals and procedural rules for common action. To achieve this, a core of the community is needed to maintain the social process within, by initiating action, generating ideas, and energising the community. Members of the core need to have specific psychological traits (engagement, motivation and charisma etc.) as well as specific structural positions in the social network. In any thriving CAP there is a hierarchy of engagement levels, where the core forms only a small fraction of the community. Even though the average member does not contribute a lot and only consumes, she is crucial to drive the motivation of the more engaged users. In fact, most contributions and products of CAPs are non-exclusive and non-subtractable goods [13] and thus free-riding is not detrimental: the more users and consumers, the better.

In summary, the engagement plans need to exploit the motivations of the potential platform users. Two main incentives for users are their own **self-benefit** from the content created by the platform, but also the feeling of the general **contribution** to society, which is again associated with the benefits of the platform and the values that it promotes. The main benefit of P_bNorms is the ability that it gives to its users to control their personal data. A third incentive is **recognition**, a basic human psychological need. People want recognition and positive feedback that acknowledges their contribution. Ranking and leaderboard mechanisms can be used to reward user activity, but also their ability to generate quality results. A fourth incentive is (non-monetary) **rewards**. Different reward mechanisms can reinforce the activity of users, e.g., free services, reputation building, privacy-related tips and tricks for each checkpoint reached etc. And a final incentive is **fun**. Setting up competitions for new content generation, or giving a social network flavour to a platform (through which users can chat or connect to other social media accounts), are some of the techniques for making the platform more appealing.

Of course, non-participation is equally acceptable, as with any other CAP. For interested users though, the strategies employed should exploit as much as possible the empirical findings observed by evaluating existing CAPs which, among others, have shown that the average user continuously needs new interaction models to maintain her interest [14].

B. Stakeholder Involvement Support

Different approaches to secure the privacy of sensitive user information have been suggested in the past, but did not make the expected impact, either because they were too complex for end-users to use or because they were never welcomed by the stakeholders. Securing the confluence of service providers is indeed a critical success factor and requires a careful balancing between the wishes of end-users and stakeholders' needs.

A challenge with privacy directives expressed as norms is that there is no guarantee that services providers will comply with the policies generated. In contrast to legislation, privacy norms are not compulsory as they only reflect the expectations

[8]http://www.w3.org/P3P/

of the community. Consequently, in order for the process to have essential impact in a society-wide scale, norms must be embraced by service providers. This can be achieved in a spirit of fairness and awareness, where all involved participants, understand that their benefits run in parallel. An advantage of explicitly characterizing the specifications of norms is not only that compliance can be verified, but also that sanctions can accompany the different types of violations. Our P_bNorms approach will rely on deploying the following persuasion strategies, presented in order of intensified pressure:

a. *Limit access, but not eliminate it*: it is clear that data sharing can significantly improve a lot of aspects of everyday life; the problem is to find the golden ratio that balances the benefits and losses for all involved parties. Norms have been successful in regulating self-governed agent societies, and various analytical and visualisation tools can raise awareness on the fitness-for-purpose of generated norms.

b. *In a competitive market, invest in trust*: a 2014 survey by the Office of the Privacy Commissioner of Canada[9] found that 81% of responders would choose services by certain firms specifically because of their privacy-friendly reputation. By advertising through communication channels the benefits that stakeholders can reap in adopting the expectations that the users themselves have specified, measurable indicators can be offered about the profits that stakeholders can gain. On the other hand, news about complaints or privacy breaches piling up can have a domino effect on a provider's reputation.

c. *Peer pressure in action*: once awareness becomes community-wide, peer pressure and coordinated actions can become a very strong parameter for cultivating a privacy-friendly behaviour by service providers. The adoption of the Do Not Track[10] option by all major Web browsers is a characteristic example. Practices, such as the story-telling engagement strategy, can allow users to share true stories about platforms and apps, making evident the available choices in the market. Coordinated surveys of selected services can further suggest changes, publicizing the results for service providers to comment upon and decide whether to comply or not.

d. *Technologically smart community reaction*: components, such as the PrivacyWiki, will make Web users aware of their privacy rights, and also offer a place for highly technologically competent community members to suggest technological solutions that offer protection. Countermeasures for apps that do not comply with their declared policies are becoming popular, and can reduce the payoff of untrustworthy providers without affecting users' experience. For example, some apps permit users to manually toggle off permission to certain PGs, while others enable the transmission of erroneous data to applications that are not supposed to collect them, lowering the quality of advertisements and statistics and leading to loss of profits for service providers.

In P_bNorms, users cannot impose their opinion on stakeholders (or vice-versa), which essentially forces both parties into a compromise maximising their mutual benefits.

[9]https://www.priv.gc.ca/information/por-rop/2015/por_2014_12_e.asp

[10]https://en.wikipedia.org/wiki/Do_Not_Track

VI. Conclusions

Privacy protection in the digital age attracts the attention of law and policy makers, as well as researchers from different disciplines. Working groups, such as the W3C Privacy Interest Group[11] and the Internet Privacy and Identity, Trust and Reputation Mechanisms (JRA5) Working Group[12] aim to understand better the problems and feed regulation and standardisation efforts. Many FP7 projects on collective awareness, such as USEMP[13] and D-CENT[14] have added privacy-related issues in their research agenda. While sharing the same starting point, the P_bNorms paradigm does not particularly focus on developing technological means to protect sensitive data, but aims to enable the involved parties to express their needs and to create processes that promote profitable and sustainable privacy policies, even for emerging or future technologies. It is clear that any solution relying on "peer pressure" needs to be appropriately coupled with the involvement of private and public units, such as NGOs. The key is to let users understand their power over their private data; they just need to use this power collectively and wisely.

References

[1] M. Weiser, "The Computer for the 21st Century," *Scientific American*, vol. 265, pp. 94–104, 1991.

[2] R. H. Sloan and R. Warner, *Unauthorized Access: The Crisis in Online Privacy and Security*, 1st ed. CRC Press, Inc., 2013.

[3] L. Haddon and S. Livingstone, "EU Kids Online: national perspectives," in *EU Kids Online, The London School of Economics and Political Science, London, UK*, 2012.

[4] F. Sestini, "Collective awareness platforms: Engines for sustainability and ethics," *Technology and Society Magazine, IEEE*, vol. 31, no. 4, pp. 54–62, 2012.

[5] T. Berners-Lee, J. Hendler, and O. Lassila, "The semantic web," *Scientific American*, vol. 284, pp. 34–43, 2001.

[6] I. Rahwan and G. R. Simari, *Argumentation in Artificial Intelligence*, 1st ed. Springer Publishing Company, Incorporated, 2009.

[7] C. Chesñevar, J. McGinnis, S. Modgil, I. Rahwan, C. Reed, G. Simari, M. South, G. Vreeswijk, and S. Willmott, "Towards an argument interchange format," *Knowledge Engineering Review*, vol. 21, no. 4, pp. 293–316, Dec. 2006.

[8] F. Bex, J. Lawrence, M. Snaith, and C. Reed, "Implementing the Argument Web," *Communications of the ACM*, vol. 56, no. 10, pp. 66–73, 2013.

[9] E. Ostrom, *Governing the commons: The evolution of institutions for collective action*. Cambridge, UK: Cambridge University Press, 1990.

[10] F. Bagnoli, A. Guazzini, G. Pacini, I. Stavrakakis, E. Kokolaki, and G. Theodorakopoulos, "Cognitive structure of collective awareness platforms," in *IEEE 8th International Conference on Self-Adaptive and Self-Organizing Systems Workshops (SASOW)*, 2014, pp. 96–101.

[11] J. C. Turner, "Towards a cognitive redefinition of the social group," in *Social identity and intergroup relations*, 1982, pp. 15–40.

[12] W. A. Kellogg and R. T. Erickson, "Social Translucence, Collective Awareness, and the Emergence of Place," in *Proc. of CSCW2002*, 2002.

[13] C. Hess and E. Ostrom, "Ideas, Artifacts, and Facilities: Information as a Common-Pool Resource," *Law and Contemporary Problems*, vol. 66, no. 1/2, pp. 111–145, 2003.

[14] L. S. G. Piccolo, H. Alani, A. De Liddo, and C. Baranauskas, "Motivating online engagement and debates on energy consumption," in *Proceedings of the 2014 ACM Conference on Web Science*, ser. WebSci '14, 2014, pp. 109–118.

[11]http://www.w3.org/Privacy/

[12]NoE in Internet Science, http://www.internet-science.eu/

[13]http://www.usemp-project.eu/

[14]http://dcentproject.eu/