The Privacy Paradox between Users' Attitudes, Stringent Legal Framework and (the Lack of) Adequate Implementation Tools

Shara Monteleone

EC, JRC-IPTS, Seville, Spain
sc0563@gmail.com, shara.monteleone@ec.europa.eu

Abstract. This paper discusses the phenomenon, typical of our Digital Age, called as the 'privacy paradox': although users are aware of the threats to their privacy, the analysis of their online behavior seemingly shows a lack of interest in their privacy, as they keep using online services and products, and even if they know their privacy rights and the existing legal measures to protect them, they appear unwilling of using available protection tools. This paper will show that the reason of this (apparent) paradox is not necessarily the users' neglectful attitude towards their privacy but should be found in the lack of effective implementation tools, at both legal and technical level (e.g. privacy policies).

Keywords: privacy paradox, European DP legal framework, privacy policies.

1 Introduction

This paper will, firstly, discuss the phenomenon called as 'privacy paradox': although users are aware of the threats to their privacy, the analysis of their online behavior seemingly shows a lack of interest in their privacy, as they keep using online services and products and even if they know their privacy rights and the existing legal measures to protect them, they appear neglecting protection tools. Secondly, it will sustain that the reason of this (apparent) paradox is not necessarily the users' neglectful attitude towards their privacy (youngsters are often accused of 'not caring' about their privacy) but should be rather found in the lack of effective implementation tools, at both legal and technical level. One of the persisting issues regarding data protection rights is the fact that, despite their the fact they are acknowledged in numerous legal acts, their practical implementation is often not feasible. This situation makes difficult for the users to fully exercise their data protection rights (the only alternative would be to quit the digital environment); meanwhile, it allows those who have the burden of providing information on the data processing they carry out and of safeguarding users' data, to easily bypass the stringent data protection rules (e.g. ISPs that provide incomplete information, or do not require users' consent while collecting their data, or create and sell profiles of unaware users). Often, the inapplicability of certain legal measures neutralizes the legal strength of the principle that stays behind them. Leaving aside the economic/ political reasons that may play a relevant role in these implementation

L. Marinos and I. Askoxylakis (Eds.): HAS/HCII 2013, LNCS 8030, pp. 284–294, 2013.

hurdles, this paper focuses on the legal and technical shortfalls of the existing data protection system, as the main problem seem still lying in the separate approaches through which the legal and technical issues, as regards privacy, are addressed.

Some scholars have already pointed out the need to achieve also in the privacy domain a more integrated legal-technical approach (Poullet 2005), and to adopt ad hoc measures, like 'Transparency Enhancing Technologies' (Hildebrandt 2008). This paper claims that the adoption of this approach is even more urgent in a developed Information Society, taking as case study the online privacy policies and their level of effectiveness as privacy-enhancing tools. Some examples of experiments and good practices are also illustrated. Finally, the opportunities/limitations of the new European Proposal for a Regulation on Data Protection, as regards the achievement of a more effective legal-technical framework, will be briefly considered.

2 Data Disclosure *vs* New Privacy Perception: The Eurobarometer's Results

In June 2011, as a result of a three years study, the European Commission published the Special Eurobarometer 359 (EB), the largest survey ever conducted in Europe on the attitudes of the European citizens regarding data protection and Electronic identity.[1] From this EB interesting data emerge about users' perceived control over their personal data, about awareness of privacy risks, expectations and disclosure habits that not necessary correspond to the common idea about people's behaviour with regard privacy protection. A general consideration that can be inferred is that the majority of people in Europe are aware of the risks raised by the use of digital technologies, but, nonetheless, they continue to disclose their personal data in their daily online activities, e.g., on social networks (SN)[2]. This 'privacy paradox' may be rethought in the light of the Eurobarometer and re-assessed as an *apparent* paradox: in other words, there is not necessarily a contradiction in the Internet users' behaviours. What might be contradictory or inadequate are, instead, the available legal and technical instruments to safeguard users' privacy and to allow them, meanwhile, to fully enjoy the advantages of innovation and technology.

In order to understand this 'apparent' paradox some example may help. The majority of Europeans see disclosing personal information as an increasing part of modern life and the social networking users are more likely to disclose their personal information. However, when we look at the reasons of disclosure, the most important

[1] See European Commission, Special Eurobarometer 359 (2011), `http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf`. and W. Lusoli, et al. *Pan-European Survey of practices, attitudes & policy preferences as regard personal identity data management*. EC JRC Institute for Prospective Technological Studies EUR- Scientific and Technical Research series, Luxemburg: Luxemburg Publications Office (2012).

[2] Similar considerations emerge from previous studies on users' privacy concerns conducted in U.S. See J. Tsai, L. Cranor, A. Acquisti, C. Fong, What's it to you? A survey of online privacy concerns and risks, Preliminary Progress Report 2006, *NET Institute Working Papers n. 06-29*.

one seems to be to access an online service (61%). From the Eurobarometer it appears that, though Internet users are commonly concerned about their privacy, they feel that it is necessary (when not mandatory) to provide personal information in order to obtain a service and almost a half of Internet users in Europe say they have been asked for more personal data than necessary when they tried to access or use an online service. A large number of Europeans (70%) are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected.

Data protection Laws in Europe and elsewhere have been strengthened against the indiscriminate practices of online companies to collect personal data and create detailed profiles over users[3]. As a response to privacy concerns, information notices (so-called privacy policies) started to be imposed by mandatory regulation (like in EU) or adopted, as self-regulation practices, by businesses (like in U.S.). The majority of Internet users report to read privacy statements. Most of them say to be informed about the data collection conditions when registering for a service online (in Europe, the 54%), appearing to have a good perception of control. However, people do not act according to their statements as they show not to read the privacy policies entirely or to find difficult to obtain information about a website's data protection practices[4].

From the point of view of the accountability, most users feels responsible themselves for the safe processing of their personal data. As for the strategies used to protect their privacy on Internet, the usual strategies are technical or procedural, like tools and mechanisms to limit spam, or checking whether a website has a safety logo that ensures a protected transaction.[5] When asked what type of regulation should be introduced to prevent companies from using people personal data without their knowledge, most Europeans think that such companies should be fined, banned from using such data, or compelled to compensate the victims. The inference is that, when users are provided with adequate privacy protective tools, or when they dispose mechanisms to better know how to avoid privacy risks, they make use of them.

Data from the Eurobarometer point out also some discrepancies in the behaviour of older and younger users, so called Digital Natives[6], with as regards a number of rele-

[3] See the European Commission Proposal for a DP Regulation of the 25 January 2012, Art 20 ("Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.") in which few exceptions are contemplated. For a first analysis of the text see P de Hert, and V Papakonstantinou, 'The proposed data protection Regulation replacing the Directive 95/45/EC: a sound system for the protection of individuals', Computer Law and Security Review 28 (2012).

[4] J. Tsai, L. Cranor, A. Acquisti, C. Fong, What's it to you? A survey of online privacy concerns and risks, Preliminary Progress Report 2006, *NET Institute Working Papers* n. 06-29, accessible at `http://papers.ssrn.com/sol3/papers.cfm?abstract_id=941708`.

[5] This emerges from the Eurobarometer 359 (2011).

[6] In literature a difference is made between Digital Immigrants and Digital Natives, the latter being, the youngsters, born and raised with digital technology (M Prensky, 'Digital Natives, Digital Immigrants', On The Horizon. 6 MCB University Press (2001). In the EB 359 (2011) they are Europeans aged 15-24.

vant issues[7]. Around 94% of the users aged 15-24 use the Internet; 84% of them use social networking sites and a large majority of them use websites to share pictures or videos. Digital Natives are also most likely to disclose various types of personal data on social networking sites; they usually do not read privacy statements/policies on the Internet but they feel sufficiently informed about the conditions for data collection and the further uses of their data when accessing a social networking site or registering for a service online. They are also more likely to feel that they have control over the information disclosed on social networking or sharing sites (84%) and they are the *least* likely to mention the risk that their data may be used to send them unwanted commercial offers or that the websites will not respect the privacy policies[8].

3 Reasons of This (apparent) Paradox

Knowing the behaviours as regards privacy, especially of young people, is important, first of all, for online companies, in particular for those like social networks that provide most of the services to teens and to advertisers (often their partners).

The way Digital Natives behave through the different services and applications existing online is, to some extent, a barometer and a driver of the success of Internet companies and the services they offer. A SN as Facebook knows it very well as it was able to progressively adapt its platform to new trends (e.g., introducing FB messanger) or to users' criticisms (changing its privacy policies) more than it did to regulators' warnings (it took FB a couple of years to disable, as ordered by the EU Data Protection Authorities, the automatic tagging relying on facial recognition features)[9].

The attitudes of young people (they are the target for many commercial companies) is also taken into account when, on the opposite, they demonstrate a changing behaviour, such as a decreased interest in a service or in the whole functioning of a SN. Behavioural studies are being run in the last years to investigate the users' response to the online tracking practices[10], as well as the response to the available privacy protection tools from which policy considerations are drawn. More recently, research pays attention also to the users' response to the personal information overload. At first, the success of SN was accompanied, especially among teenagers, with an over-disclosure trend (in contrast with the legal requirement and good practice of data minimization).

---

[7] Similar survey conducted outside Europe is that of: Hoofnagle et al., *How different are Young adults from older adults when it comes to information privacy attitudes and policies* Survey, April 14, 2010.

[8] See the Eurobarometer 359, p. 7; 204.

[9] See S. Monteleone, Privacy and Data Protection at the time of facial recognition: towards a new right to digital identity?, European Journal of Law and Technology, Vol 3, n 3, 2012. N. Andrade, A. Martin, S. Monteleone, "All the Better to See You with, My Dear": Facial Recognition and Privacy in Online Social Networks, in *IEEE, Security and Privacy*, 99 2013.

[10] A. Acquisti, J Grossklags, What Can Behavioral Economics Teach Us About Privacy? In *Digital Privacy: Theory, Technologies and Practices*, Taylor and Francis Group, 2007; N. King, P. Wegner Jessen, Profiling the mobile customer – Privacy concerns when behavioural advertisers target mobile phones, *Computer Law and Security Review,* 25, 2010.

A SN like FB has been, so far, the place where to share pictures, tell stories about oneself, look at the others' profiles and 'brag' about one's everyday little achievements. However, the euphoria of the first moment seems to be replaced by a colder attitude towards the over-sharing social networking system. Though few data exist at the moment[11], it is possible that "the age of overshare…the age of brag is over".[12] Knowing what is the favorite SN of contemporary users is not the aim of this paper; however, what these new trends testify is that users start to prioritize privacy to data disclosure.

Not only DN have shown a different behaviour in terms of privacy online if compared to their parents, revealing in many case a different privacy perception[13]rather than a disregard for their personal data. They seem to have changed their same preferences as regards SN or other on-line services but more important the web community is changing and perhaps privacy need starts to be more important for young people.

This would also explain why a very popular social network like FB, as today's press reports[14], is starting to lose appeal among young people bored of the information overload and the over-exposition of themselves and friends; on the opposite, younger users seem to be more projected towards new Apps or sites (like Tumblr) that offer them a more intimate way to communicate or share (e.g., only with few, trusted people). It appears not only a question of social trends among youngsters (looking for the coolest apps) but also a question of privacy preference and identity construction. They simply may want more privacy[15].

Though young people may ignore (and it is not always the case) the risks of being tracked, of the data usage made by their favorite website, of the profiling for marketing purposes, they seem however to have started to naturally move towards "contextual social networks", more restricted platforms apt to truly shared interests[16], as well as to prefer privacy protective websites (like Tumblr, with its simple privacy

[11] See the Pew Internet Report on a survey conducted by the Pew Research Center that shows, if not a mass abandon to FaceBook but more a fragmentation and a shift in the behaviour of FB users, who have taken breaks from using the site in the last years (61%) and who plan to spend less time on the SN during the 2013 (an almost 40% of young users). Notable numbers point to a decreasing value and a decline in usage over the past year. The report contains also data about the Tumblr's success: `http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_Coming_and_going_on_facebook.pdf`

[12] E. Hamburger, The age of the brag is over: why Facebook might be losing teens, The Verge, 1/03/2013.

[13] S. Monteleone, N. Andrade, Digital Native and the metamorphosis of the European Information Society, The Emerging Behavioural Trends Regarding Privacy and Their Legal Implications in S. Gutwirth et al. *Data Protection: Coming of Age*, pp 119-144.

[14] See V. Luckerson, "Is facebook losing its cool? Some teens think so" Time, Business & Money, 7 March 2013.

[15] The reasons for the success of a social network like Tumblr seems to lie, in fact, in the possibilities it offers to build/create two or more digital identities, as opposed to FB's one (and often real) identity.

[16] As it has been observed, companies like Facebook and Twitter "have turned their focus away from users and toward shareholders to get bigger, not better", this being also the reason why they are anymore in the list of the most innovative companies, see D. Lidsky, Fastcompany.com `http://www.fastcompany.com/most-innovative-companies/2013/why-facebook-and-twitter-are-not-most-innovative-companies`

policies). The private sharing seems also to be at the basis of the success of a mobile App like Snapchat and its temporary service (where photos last about only 10 seconds): as it has been observed, in our age, "where a sense of online privacy is very sacred, being able to communicate without leaving a permanent record is empowering".[17]

4 Legal and Technical Issues: Different Approaches

FB and like are called to be more agile and to adapt to the new trends; but the change is not only on this side. The new trends and changing attitudes of users with regards to their data protection are also relevant for law-makers, first, because the users' behavior (e.g., reading or ignoring the privacy policies) may impact the implementation degree of a legal requirement, such as the information obligation borne by the service provider; but also because users' behaviour, especially of DN, tell us a lot of the evolving needs of users, that cannot be ignored by a DP regulation that wants to keep pace with the times, and it obliges us to (re-)think about legal-technical responses.

The law should be attentive to the techno and socio-economic trends regarding information and communication technologies and flexible enough to adapt to new relevant changes that occur in the society (more and more merely 'Information' society), to support the technological development and (not less important) to allow the users to be more free in their preferences as regards privacy protection, at least in situations in which the rigid intervention of the law risks to result in an excess of paternalism, being sometimes dangerous instead of beneficial for the users' rights.

If the Law cannot precisely anticipate the technological trends it should at least become able to have a prospective vision of the users' attitudes and needs as regards their data protection and identity management[18]. It should be able not to fossilize itself in outdated mindsets and requirements but evolving with the technologies as the users' rights are to be benefited through the technology; it should be able to forecast what it is opportune to strictly regulate and what not, also according to what users and in particular DN manifest. Meanwhile, regulation should be firm on sensitive legal issues concerning data protection, like the unauthorized re-use of personal data, illicit data access, sensitive data processing and accountability issues.

5 The Case of the Privacy Policies

As previous studies pointed out[19], by lowering the barriers to finding privacy information, i.e., to making the access to privacy policies easier, simpler, agile and therefore more effective, users may be able to take more informed decisions regarding the usage of their personal information online. The current existing privacy policies are not effective, as surveys demonstrated, though allow companies to easily demonstrate they are compliant with privacy regulations.

---

[17] E. Hamburger, The age of the brag is over: why Facebook might be losing teens, The Verge, 1 March 2013.

[18] See S Muller, S Zouridis, M Frishman and L Kistemaker**,** The Law of the future and the future of Law, TOAEP, 2012.

[19] J. Tsai, L. Cranor, A. Acquisti, C. Fong, What's it to you? A survey of online privacy concerns and risks, Preliminary Progress Report 2006, *NET Institute Working Papers* n. 06-29.

The new European Proposal for Data Protection Regulation aims at strengthening the individual rights also imposing the transparency principle as a rule[20]. How to make these privacy notices more effective? Should the law impose stricter requirements for privacy policies of online providers? A similar approach might probably help users to be more aware of the usage that third parties make of their data and to be able to protect better their privacy (i.e. to limit the data disclosure); nevertheless, stricter legal requirements on how a privacy notice should appear/should what contain, would probably be countered by companies that would see them a further burden (unless they receive incentives to adopt them and the technology proposes simple and cheap solutions). Without counting the fact that those who have at the end to pay the price of this burden will be probably the same end-users, in a way or another.[21]

However, as it emerges from recent press[22], online privacy is not only imposed by regulators and urged by privacy advocates, but it became an achievement to purse for business, an asset to flaunt in competition with each other that can make the market advantage. Given that people are more and more concerned about their privacy as technology becomes an essential part of their daily life, the race among companies to convince the consumers that their data are safe is, in some ways, proving to be an effective competition driver, fruitful not only for the market but for the same privacy goals. This is especially true in the U.S. [23], where there is not a general DP Law and

[20] See Art 11 of the European Proposal for a general DP Regulation: "1.The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights. 2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child."

[21] A different issue is that related to the nature and level of regulation that would better suit with the aim of imposing precise information notices in view of protecting users' privacy. Would this role be better played at national or supranational level in order to regulate data processing, ensuring the safeguard of individual privacy rights and meanwhile the economic growth (increasingly relying in data-intensive business models)? Would a state-mandatory regulation be the best choice for this purpose or self-regulation mechanism or co-regulation strategies would better serve this scope? Lively debates around these issues take place in legal and non legal environments.

[22] S. Sengupta, 'Web privacy becomes a business imperative', *TheNewYorkTimes*, March 3, 2013.

[23] For instance, Apple started to require applications in its operating system to get permission from users before tracking their location; Microsoft turned on an anti-tracking signal in its browser, Internet Explorer, and Mozilla more recently announced that it will soon allow its users to disable third parties tracking software; moreover, the businesses have also started to provide some specific mechanisms that allow users to better control their data, like Google Plus's 'Circles', a way to keep separate sharing spaces and a context-sensitive social network. See on this: S. Sengupta,'Web privacy becomes a business imperative', *TheNewYorkTimes*, March 3, 2013. However, Google had also recently faced the strong reactions of EU Data protection Authorities after its decision to shift its privacy policies, to integrate all its products/services so to be able to collect, combine and store users data across all its online services; see on this: L. Essers, EU privacy taskforce plans to take action against Google before the summer, *Infoworld* 28 February 2013 (CNIL press release at: `http://www.cnil.fr/english/news-and-events/news/article/googles-privacy-policy-g29-ready-for-coordinated-enforcement-actions/`)

where the recent attempts to curb online companies with binding privacy rules did not seem to be so far particularly successful[24]. In these conditions, the fact that companies develop privacy protecting services is also a way for companies to avoid state strict regulation. However, proposing more effective privacy-friendly mechanisms is a competitive plus for a company and fosters the development of more privacy protective tools. Said that, a question that may rise is whether the online companies should be left free to decide how to shape their privacy policies, according to a self-regulation model, instead of imposing them government restrictions on privacy[25].

What if it is, on the opposite, a mere technical problem? In this case, would the designers of technical privacy-enhancing solutions be the sole accountable for the protection/breach of individual privacy?

6 Joint Responses: Towards a Renewed Legal-Technical Approach

The right approach is not easy to seek, but it does not seem to have a unidirectional nature[26]. In particular, the EU policy challenge in this field will be to conciliate its classical fundamental rights approach with a more technological or market-driven one[27]. Probably the reasons of inadequate responses available so far are to be found in the fact that legal and technical issues have been addressed as two completely separate fields, though a legal-technical approach to privacy problems has been urged

[24] The reference is in particular to the Do Not Track systems launched a couple of years ago in the U.S. DNT is a browser setting that would allow Internet users indicate that they do not want their activities to be tracked, but no consensus has been reached among privacy advocates, Internet companies and online advertisers. See J Melvin, Do not Track Internet spat risks legislative crackdown, *Business News,* 24/07/2012. However, a new bill, aimed to ensure that web browsers and online companies provide users with opt-out options of being tracked by advertisers, has been recently introduced in the U.S. Senate, See D. Kerr, Do Not track privacy bill reintroduced in Senate, CNET News, 28/02/2013.

[25] This kind of question arose for instance in the occasion of the recent launch of the 'privacy lockers'. The underlying principles are in line with a propriety rights approach of personal data, as they assume that a data-subject is the 'owner' of her data-assets, who can decide (and transact) about their use. A market of personal data management tools is already emerging. These start-up companies, that promise to work as data lockers are Azigo, Mydex, the Data Banker, Personel.com, Connect.me. They work as cyber-lockers that would allow users to store own personal data and meanwhile as personal digital assistant.

[26] See Y. Welinder. A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks. *Harvard Journal of Law and Technology*, 26(1):165-239, 2012, who stressed that even good market-based solutions should to be considered possible only in combination with legal (i.e. consent and information notice requirements) and technological ones (i.e., privacy-by-design/notices).

[27] Legal studies have already demonstrated that the adoption of a property-oriented vision of personal data also in Europe is not only formally possible, but that offers also advantages in solving data protection issues, see: N. Purtova, *Property Rights in Personal Data. A European perspective*, Kluwer Law International 2012.

since years[28]. Several scholars stressed that many privacy concerns may be addressed through a good design that embeds fundamental privacy principles[29].

Some good examples of experiments and studies are not missing as mentioned below. However, political resistances or practical difficulties prevent their adoption. Examples of the implementation of a legal-technical approach, better called as privacy by design[30], are, for instance, the privacy agents studied for online environments or for the more concealed data processing carried out in ubiquitous computing (Ambient Intelligence)[31]. Similar to these agents are the tools ideated to make privacy policies more accessible[32] or more effective by increasing their interactive nature (like the 'visceral notices')[33]. Other studies, for instance in behavioural economics, propose the introduction of (tested) tools like 'privacy nudges' for behavioural advertising, location sharing and social networks.[34]An example of techno-legal mechanism, introduced recently in Europe, that has also an economic impact, is the 'privacy seal'.[35]

The problem with many of these solutions is that their implementation may be difficult in practice and burdensome for businesses.

---

[28] Y. Poullet (2005). Pour une troisième génération de réglementations de protection de données, *Jusletter*, 3 (22); M. Hildebrandt (2008c), Legal and technological normativity: more (and less) than twin sisters, *Techné: research in philosophy and Technology,* 12, 3, who sustains, however, that technological devices should be regulated by the law, "precisely because they are able to regulate and constitute our interactions".

[29] T Olsen, and T Mahler, 'Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust''. Computer Law and Security Report*, 23,* (4&5) 2007; A Murray, Information Technology Law. The Law and Society, Oxford University Press (2010); on the concepts of 'Transparency Enhancing Technologies' (allowing citizens to anticipate how they will be profiled and the consequence of that) see M. Hildebrandt (2012). Hull, G, Lipford, HR and Latulipe C (2011), 'Contextual Gaps: Privacy issues on Facebook', Ethics and Information Technology, 4; S. Monteleone, 'Privacy and Data Protection at the time of Facial Recognition: towards a new right to Digital Identity?' European Journal of Law and Technology, 3/3, `http://ejlt.org//article/view/168/257`

[30] See A. Cavukian, Privacy by design and the emerging personal data ecosystem, October 2012. `http://www.ipc.on.ca/images/Resources/pbd-pde.pdf`

[31] D Le Métayer, S Monteleone. Automated consent through privacy agents: Legal requirements and technical architecture. *Computer Law & Security Review,* Elsevier, 25(2), 2009. L. F. Cranor, User Interface for privacy agents in *ACM TOCHI*, vol 13, 2, 2006.

[32] See for instance, the Privacy Finder (a privacy-enhanced search engine) described in J. Tsai, L. Cranor, A. Acquisti, C. Fong, What's it to you? A survey of online privacy concerns and risks, Preliminary Progress Report 2006, *NET Institute Working Papers n. 06-29*. The ability of this privacy-enhanced search engine (a P3P tool) to provide information that address privacy concerns is explored by Tsai et al., who conclude that privacy concerns and risks may be mitigated through the design of tools that make online privacy notices more accessible and easy to find.

[33] R. Calo, Against notice scepticism in privacy (and elsewhere), *87 Notre Dame Law Review* (2012).

[34] A. Acquisti, From the Economics to the Behavioral Economics of Privacy: A Note, in *Ethics and Policy of Biometrics*, 6005, Springer, 2010.

[35] See for instance the IXquick search engine, the first to receive the EU privacy seal `https://www.ixquick.com/eng/protect-privacy.html`

If we look at the adequacy of the European legal framework, especially in view of the criticisms received by online businesses to its ongoing reform, we should consider what the Art 29 Working Party has affirmed: despite the emergence of new technologies and globalization, the core principles of European data protection are still valid, but "the level of data protection in the EU can benefit from a better application of the existing data protection principles in practice".[36] In other words, what we miss as users are not principles and values but more suitable, interactive and effective privacy tools, able to embed in the same technological design data protection rules, but also capable to keep pace with the times.

With the aim to tackle some of these issues, the study 'Behavioural responses to online tracking and profiling' are being undertaken at the IPTS, JRC of the European Commission[37], the results of which are expected to be published in 2014.

References

1. Acquisti, A.: From the Economics to the Behavioral Economics of Privacy: A Note. In: Kumar, A., Zhang, D. (eds.) ICEB 2010. LNCS, vol. 6005, pp. 23–26. Springer, Heidelberg (2010)
2. Andrade, N., Martin, A., Monteleone, S.: All the Better to See You with, My Dear: Facial Recognition and Privacy in Online Social Networks. In: IEEE, Security and Privacy, vol. 99 (2013)
3. Andrade, N., Monteleone, S.: Digital Native and the metamorphosis of the European Information Society, The Emerging Behavioural Trends Regarding Privacy and Their Legal Implications. In: Gutwirth, S., et al. (eds.) Data Protection: Coming of Age, pp. 119–144
4. Calo, R.: Against notice scepticism in privacy (and elsewhere), 87 Notre Dame Law Review (2012), http://cyberlaw.stanford.edu/files/publication/files/ssrn-id1790144.pdf
5. Cavukian, A.: Privacy by design and the emerging personal data ecosystem (October 2012)
6. Cranor, L.F.: User Interface for privacy agents in ACM TOCHI 13(2) (2006)
7. Essers, L.: EU privacy taskforce plans to take action against Google before the summer. Infoworld (February 28, 2013), http://www.infoworld.com/d/security/eu-privacy-taskforce-plans-take-action-against-google-the-summer-213675
8. European Commission, Special Eurobarometer 359 (2011), http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
9. Hildebrandt, M.: Legal and technological normativity: more (and less) than twin sisters. Techné: Research in Philosophy and Technology 12(3) (2008c)
10. Hoofnagle, et al.: How different are Young adults from older adults when it comes to information privacy attitudes and policies Survey (April 14, 2010), http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf

[36] Article 29 WP, "The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", 2009a.

[37] http://is.jrc.ec.europa.eu/pages/Mission.html.

11. Le Métayer, D., Monteleone, S.: Automated consent through privacy agents: Legal requirements and technical architecture. Computer Law & Security Review 25(2) (2009)
12. Melvin, J.: Do not Track Internet spat risks legislative crackdown. Business News (July 24, 2012)
13. Monteleone, S.: Privacy and Data Protection at the time of Facial Recognition: towards a new right to Digital Identity? European Journal of Law and Technology 3(3), http://ejlt.org//article/view/168/257
14. Muller, S., Zouridis, S., Frishman, M., Kistemaker, L.: The Law of the future and the future of Law. TOAEP (2012)
15. Murray, A.: Information Technology Law. The Law and Society. Oxford University Press (2010); Hildebrandt, M.: (2012); Hull, G., Lipford, H.R., Latulipe, C.: Contextual Gaps: Privacy issues on Facebook. Ethics and Information Technology 4 (2011), http://ssrn.com/abstract=1427546
16. Olsen, T., Mahler, T.: Identity management and data protection law: Risk, responsibility and compliance in Circles of Trust. Computer Law and Security Report 23(4&5) (2007), http://dx.doi.org/10.1016/j.clsr.2007.05.009
17. Poullet, Y.: Pour une troisième génération de réglementations de protection de données. Jusletter 3(22) (2005)
18. Purtova, N.: Property Rights in Personal Data. A European perspective. Kluwer Law International (2012)
19. Sengupta, S.: Web privacy becomes a business imperative. TheNewYorkTimes (March 3, 2013), http://www.nytimes.com/2013/03/04/technology/amid-do-not-track-effort-web-companies-race-to-look-privacy-friendly.html?pagewanted=all&goback=%2Egde_4255573_member_219668331&_r=0
20. Tsai, J., Cranor, L., Acquisti, A., Fong, C.: What's it to you? A survey of online privacy concerns and risks, Preliminary Progress Report 2006, NET Institute Working Papers n. 06-29, accessible at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=941708
21. Welinder, Y.: A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks. Harvard Journal of Law and Technology 26(1), 165–239 (2012)