Agentschap voor Innovatie door Wetenschap en Technologie
IWT
SBO Security and Privacy for Online Social Networks

Document type	Report
Title	Policy Recommendations for Privacy-Friendly Social Networks
Deliverable Number	D9.6.6
Authors	Valerie Verdoodt, Brendan Van Alsenoy, Ellen Vanderhoven and Ralf De Wolf
Dissemination level	Public
Preparation date	26 February 2015
Version	1.0

The IWT SBO SPION Project

Nr.	Participant name	Country	Department	Participant role
1	KU Leuven	BE	COSIC/ESAT	Coordinator
2	KU Leuven	BE	DISTRINET	Partner
3	KU Leuven	BE	DTAI	Partner
4	KU Leuven	BE	ICRI	Partner
5	Vrije Universiteit Brussel	BE	SMIT	Partner
6	Univerity of Ghent	BE	OWK	Partner
7	Carnegie Melon University	USA	Heinz	Partner

Contributors

	Name	Organisation
1	Valerie Verdoodt	ICRI, KU Leuven - iMinds
2	Brendan Van Alsenoy	ICRI, KU Leuven - iMinds
3	Ellen Vanderhoven	OWK, University of Ghent
4	Ralf De Wolf	iMinds-SMIT, VUB

1. INTRODUCTION 4

2. EDUCATION AND AWARENESS 5

2.1 A SAFER INTERNET 5
2.2 THE ROLE OF SCHOOLS 6
2.3 RECOMMENDATIONS 7

3. AT THE LIMITS OF "NOTICE & CONSENT" 11

3.1 WHY NOTICE? 11
3.2 REGULATORY FAILURE 11
3.3 RECOMMENDATIONS 12

4. DEFAULT MATTERS 14

4.1 THE "POWER OF DEFAULT" 14
4.2 PRIVACY AND DATA PROTECTION BY DEFAULT 15
4.3 RECOMMENDATIONS 16

5. UNITED WE STAND 18

5.1 THE POWER OF COLLECTIVE ACTION 18
5.2 CURRENT MECHANISMS 19
5.3 RECOMMENDATIONS 20

6. PETS MAKE GOOD COMPANIONS 22

6.1 PETS AND PRIVACY BY DESIGN 22
6.2 NO PETS ALLOWED? 23
6.3 RECOMMENDATIONS 24

7. CONCLUSION 26

1. INTRODUCTION

The rise of social media has been one of the most significant developments in the online environment in recent years.[1] More and more individuals make use of Online Social Networks (OSNs) to stay in touch with family and friends, to engage in professional networking or to connect around shared interests and ideas. The increased availability of personal data online, as well as its accompanying metadata, has given rise to new challenges and concerns regarding privacy and security.

Our recommendations highlight several ways in which policymakers can help mitigate privacy and security risks related to OSNs. It describes a variety of approaches, ranging from education and awareness to promotion of privacy-enhancing technologies. The recommendations focus on empowering users, while at the same time enhancing the responsibility and accountability of OSN providers.

[1] O. Tene, 'Privacy: the new generations', *International Data Privacy Law* 2011, Vol. 1, No. 1, p. 22.

2. EDUCATION AND AWARENESS

2.1 A Safer Internet

Children and youngsters are amongst the largest user groups of online and mobile technology in Europe.[2] OSNs offer them an attractive means for communication, socialisation and information.[3] They promote the shaping of identity[4] and enhanced participation of individuals in political, social and cultural life.[5] Unfortunately, the use OSNs brings with it certain risks. Children and youngsters may be exposed to online risks such as (cyber-) bullying, sexting, exposure to harmful content, privacy harms, but also commercial risks.[6]

Given these challenges, policymakers all over the world have increased their efforts to promote a safer Internet for children and youngsters.[7] In 1999, the European Commission launched the first **Safer Internet Programme**, with a view to

> "*empower and protect young people online, by promoting a safe and responsible use of Internet and other communication technologies and by fighting illegal and harmful online content and conduct.*"

In 2009, The European Commission brought together OSN providers and civil society organisations to discuss how to enhance the safety of children and young people using OSNs. This cooperation resulted in the **Safer Social Networking Principles for the EU,** which highlighted the important role of "parents, teachers and other carers" in educating children about safe and responsible online behaviour.[8]

---

[2] European Commission, "From a Safer Internet to a Better Internet for Kids" http://ec.europa.eu/digital-agenda/en/safer-internet-better-internet-kids (last accessed 12 February 2015)

[3] V. Donoso and V. Verdoodt, "White Paper Social media literacy: Time for an update!", EMSOC Project, 2014, 6, available on http://emsoc.be/5720-emsoc-white-paper-social-media-literacy-time-for-an-update/.

[4] E. Vanderhoven, "Raising risk awareness and changing unsafe behavior on social network sites: A design-based research in secondary education", Proefschrift ingediend tot het behalen van de academische graad van Doctor in de Pedagogische Wetenschappen, UGent, 2014, 231; V. Donoso and V. Verdoodt, *o.c.*, 6.

[5] Council of Europe, Recommendation on the protection of human rights with regard to social networking services, 4 April 2012, available on https://wcd.coe.int/ViewDoc.jsp?id=1929453&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

[6] G. Mascheroni and K. Ólafsson, "Net Children Go Mobile: risks and opportunities", Milano, Educatt, 2014, 5, 91; S. Livingstone, "Developing social media literacy: How children learn to interpret risky opportunities on social network sites", *Communications* 2014, 39 (3), 283-303, as cited by V. Donoso and V. Verdoodt, *o.c.*, 14.

[7] Council of Europe, Recommendation on the protection of human rights with regard to social networking services, 4 April 2012, available on https://wcd.coe.int/ViewDoc.jsp?id=1929453&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383; European Commission, Safer Internet Programme, 1999; European Commission, Communication on a European Strategy for a Better Internet for Children, 2 May 2012, available on https://ec.europa.eu/digital-agenda/en/news/communication-european-strategy-make-internet-better-place-kids.

[8] Safer Social Networking Principles for the EU, 10 February 2009, accessible at https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf.

More recently, the European Commission's Digital Agenda for Europe established a new policy framework for enhancing the **digital and media literacy** of social media users. This framework includes a strategy for a Better Internet for Children which emphasises that:

> "*Children, their parents, carers and teachers need to be aware of the risks children can encounter online as well as of the tools and strategies to protect themselves or cope with such risks. Children need to develop their critical thinking and digital and media literacy skills to be able to actively contribute in a participatory society. They need access to and advice on how to use tools suited to their age that would help them act safely and responsibly online*".[9]

Digital and media literacy skills are necessary to reap the full benefits OSNs have to offer.[10] For this reason, a right to internet and media literacy was introduced by the Draft Council of Europe "Guide on Human Rights for Internet Users" and media literacy was recognised as a key requirement for protecting human rights in an OSN context. [11] In the same vein, the European Council of Ministers and the European Commission have called to

> "*step up the implementation of strategies to include the teaching of online safety and digital competences in schools, encourage the use of the Internet across school subjects and in this respect support adequate teacher training*."[12]

2.2 The role of schools

Schools are **best positioned** to reach the majority of all children regardless of their age, background or socio-economic status.[13] They can introduce internet safety in a pedagogic context that allows for solid learning over time.[14] The European Commission recognises the importance of the role of education in its strategy for a Better Internet for Children, which includes "*scaling up awareness and empowerment through digital*

[9] European Commission, Communication on a European Strategy for a Better Internet for Children, 2 May 2012, 8.
[10] V. Donoso and V. Verdoodt, "White Paper Social media literacy: Time for an update!", EMSOC Project, 2014, 13, available on http://emsoc.be/5720-emsoc-white-paper-social-media-literacy-time-for-an-update/.
[11] Draft Guide on Human Rights for Internet Users, Council of Europe, 22 October 2013, available on http://www.coe.int/t/informationsociety/Rights%20of%20Internet%20Users/Draft%20Council%20of%20Europe%20Guide%20on%20Human%20Rights%20for%20Internet%20Users.pdf; Recommendation on the protection of human rights with regard to social networking services, Council of Europe, 4 April 2012, available on https://wcd.coe.int/ViewDoc.jsp?id=1929453, as cited by V. Donoso and V. Verdoodt, *o.c.*, 14.
[12] Council conclusions of 26 November 2012 on the European strategy for a Better Internet for Children, *O.J.* 19 December 2012, available on http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012XG1219%2804%29.
[13] European Commission, Communication on a European Strategy for a Better Internet for Children, 2 May 2012, 8.
[14] S. Livingstone, L. Haddon, J. Vincent, G. Mascheroni and K. Ólafsson, *Net Children Go Mobile. The UK report*, London, London School of Economics and Political Science, 2014, 6.

literacy and online safety in all EU schools" as one of its main objectives.[15] Both parents and children have indicated that they consider the school environment as an important place to receive information about online safety.[16] In this regard, the Council of Europe has urged its Member States to:

> "*foster awareness initiatives for parents, carers and educators to supplement information provided by the social networking service, in particular in respect of much younger children when they participate in social networks*".[17]

The educational agenda of schools is broad and generally aimed at preparing pupils for the public life.[18] More in particular, their task includes **raising awareness of e-safety** among pupils and offering guidance and training in **responsible Internet use**, including the use of OSNs.[19] Research has shown that children and youngsters are better at finding information online than they are at avoiding some of the risks they are faced with.[20] This is why e-safety, digital and media literacy have formally made it into school curricula in many European countries.[21] In addition, other entities (e.g., youth organisations) can be a valuable and fruitful environment to raise awareness and educate youngsters regarding responsible internet use.[22]

2.3 Recommendations

Make media literacy and online safety an effective component of school curricula.

Even though media literacy and online safety is formally included in the school curriculum, current implementation is **inconsistent or non-existent** in a lot of schools.[23] The problem here is that the curriculum only mentions target objectives on a macro level, which are vague and do not define the concrete content of courses or give

---

[15] European Commission, Communication on a European Strategy for a Better Internet for Children, 2 May 2012,

[16] B. O'Neill and E. Staksrud, *Final recommendations for policy*, London, EU Kids Online, LSE, September 2014, 13, 17 available on http://eprints.lse.ac.uk/59518/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_EU%20Kids%20Online_EU_Kids_Online_Final%20recommendations%20Sep%202014.pdf.

[17] Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the protection of uman rights with regard to social networking services

[18] E. Vanderhoven, *o.c.*, 119.

[19] B. O'Neill and E. Staksrud, *o.c.,* 16.

[20] S. Livingstone, "What is media literacy?", *Intermedia* 2004, 32 (3), pp. 18-20, available on http://eprints.lse.ac.uk/1027/.

[21] E. Vanderhoven, *o.c.*, 12. In Flanders, media literacy has been formally included in the curriculum of secondary education. See I. Vos and D. Terryn, *Charting Media and Learning in Europe*, MEDEANET Project, 2013, http://www.medeanet.eu/sites/default/files/MEDEAnet_Deliverable_4.3_Annual_Report_2013.pdf.

[22] R. De Wolf, K. Willaert and J. Pierson, "Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook "*Computers in Human Behavior* 2014, Vol. 35, 444-454.

[23] Safer Internet Programme, Assessment report on the status of online safety education in schools across Europe, 2009, as cited by E. Vanderhoven, o.c., 13.

insights into how these objectives are to be attained.[24] As a result, implementation at the classroom level of online safety appears to be inconsistent.[25]

To overcome these issues, efforts to ascertain equality of access and opportunities for all children are necessary. Furthermore, government should support schools and provide them with **sufficient resources** for the development of pupils' digital and media literacy skills.[26] In addition, the actual implementation of the online safety curriculum would benefit from **more guidance on the concrete content of courses**.

Promote ICT training among teachers and encourage peer-to-peer learning.

Teachers can benefit from training on both the opportunities and the challenges of OSNs. As a result, certain scholars recommend that the **development of digital skills** should become a compulsory component of teacher training programmes.[27] At the moment, teacher training programs are mostly focused on reproducing current educational models and classroom didactics.[28] However, the use of OSNs might reverse this trend, as it offers opportunities for peer-to-peer learning. Teachers-in-training can exchange experiences online and learn from others' best practices all over the world.[29] Even though such networks and online resources are already widely available in Europe, only a minority is exploiting the benefits they have to offer. [30] Therefore, government should support the sharing of knowledge and educational materials among the teaching community. Teacher training should not necessarily focus (only) on making the teachers themselves more tech-savvy. Perhaps even more important is that teachers are educated as to what it means for youngsters to be active on an OSN, so they can understand the benefits and risks from their perspectives. The latter approach also facilitates the communication between teachers and their students. In other words: developing digital skills consists of both technical and social components.

---

[24] R. Vanderlinde, J. van Braak and R. Hermans, "Educational technology on a turning point: Curriculum implementation in Flanders and challenges for schools", *Educational Technology Research and Development*, *57*(4), 573-584, as cited by E. Vanderhoven, *o.c.*, 12.

[25] Safer Internet Programme, Assessment report on the status of online safety education in schools across Europe, 2009, as cited by E. Vanderhoven, o.c., 12.

[26] B. O'Neill and E. Staksrud, "Policy implications and recommendations: Now what?" in S. Livingstone, L. Haddon, & A. Görzig (Eds.), *Children, risk and safety on the Internet. Research and policy challenges in comparative perspective* (1st ed., Vols. 1–26, Vol. 26), Bristol/Chicago: The Policy Press, as cited by E. Vanderhoven, *o.c.*, 223.

[27] B. O'Neill and E. Staksrud, *Final recommendations for policy*, London, EU Kids Online, LSE, September 2014, 17, available on http://eprints.lse.ac.uk/59518/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_EU%20Kids%20Online_EU_Kids_Online_Final%20recommendations%20Sep%202014.pdf.

[28] V. Donoso and V. Verdoodt, "White Paper Social media literacy: Time for an update!", EMSOC Project, 2014, 28, available on http://emsoc.be/5720-emsoc-white-paper-social-media-literacy-time-for-an-update/.

[29] V. Donoso and V. Verdoodt, *o.c.*, 29.

[30] European Schoolnet and University of Liège, "Survey of Schools: ICT in Education, Benchmarking Access, Use and Attitudes to Technology in Europe's Schools, February 2013, available on https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/KK-31-13-401-EN-N.pdf.

Efforts should also be made to **improve** the **quality and consistency** of ICT training across institutions. Teachers often require ongoing support for the implementation of ICT into their teaching and learning. For instance, ICT coordinators in school could provide the necessary pedagogical and technical guidance on a permanent basis.[31]

Finally, keeping programmes and teachers' up-to-date is a challenge. Technologies develop much faster than the school curriculum, study programmes and materials. Therefore a **sustainable model for training** of teachers should be developed. This would imply the continuous training and cooperation with experts (e.g. researchers, awareness or e-safety centers etc.).[32]

Evaluate the practical implementation of educational programmes about online safety.

Educational prevention programmes are aimed at enhancing awareness of OSN risks and providing information of available countermeasures. In this regard, Insafe - the European network of safer Internet centres - developed a number of prevention and awareness campaigns and materials.[33] However, research has shown that campaigns on their own do often not achieve their goals, probably because they do not always have a theoretical basis or are not evidence-based.[34] Whereas governments tend to invest in the development of educational material and campaigns, no resources are allocated to assessment or evaluation of such campaigns.[35] Consequently, it is unclear whether these initiatives have the desired impact on youngsters or what is needed in order to have a positive effect. Therefore, it is crucial that efforts are made to assess existing prevention programmes about online safety, instead of merely supporting the development of new ones.[36]

---

[31] *Idem.* However it should be kept in mind here that at the moment, ICT coordinators usually lack pedagogical and e-safety knowledge. Therefore ICT coordinators should receive specific pedagogical training, it cannot merely be an ICT technician.

[32] The Media Coach initiative funded by the Flemish government and Evens Foundations can serve as an example. See http://www.linc-vzw.be/projecten/mediacoach-een-mediawijs-traject-voor-professionelen.

[33] Insafe is "a European network constituted by 30 national Safer Internet Centres in EU Member states and in Iceland, Norway and Russia. Every national Centre implements awareness and educational campaigns, runs a helpline, and works closely with youth to ensure an evidence-based, multi-stakeholder approach to creating a better internet." See http://www.saferinternetday.org/web/guest/about. See also Insafe, "Educational resources for teachers", 2014, available on http://lreforschools.eun.org/web/guest/insafe.

[34] F. Mishna, C. Cook, M. Saini, M.-J. Wu and A. MacFadden, R., Interventions to prevent and reduce cyber abuse of youth: A systematic review. *Research on Social Work Practice*, *21*(1), 2010, 5–14 as cited by E. Vanderhoven, *o.c.*, 231. See also Vanderhoven, E., Raes, A. & Schellens, T. (2015). Interpretation in the process of designing effective learning materials: A design-based research example. In Smeyers, P., Bridges, D., Burbules, N., & Griffiths, M. (Eds.). (2015). International handbook of interpretation in educational research methods (2 Vols.). Dordrecht: Springer. Doi: 10.1007/978-94-017-9282-0_60

[35] S. Livingstone and M. E. Bulger, "A global agenda for children's rights in the digital age. Recommendations for developing UNICEF's research strategy", London, LSE, 2013, 20, 22.

[36] E. Vanderhoven, *o.c.*, 223.

Stimulate media and industry engagement for raising awareness of online safety.

Educators are not solely responsible for raising awareness about online safety.[37] First of all, general media, such as television or newspapers, can help to raise awareness. These awareness-raising activities could benefit from a cooperation between the media industry and academia, as the latter can provide guidance and evidence-based research.[38] In addition, the industry must recognize it has a responsibility of its own in providing a safer online environment for children and raising awareness of online safety.[39]

[37] E. Vanderhoven, *o.c.*, 224.

[38] V. Donoso and V. Verdoodt, "White Paper Social media literacy: Time for an update!", EMSOC Project, 2014, 41, available on http://emsoc.be/5720-emsoc-white-paper-social-media-literacy-time-for-an-update/.

[39] O'Neill and Staksrud, "Policy implications and recommendations: Now what?" in S. Livingstone, L. Haddon, & A. Görzig (Eds.), *Children, risk and safety on the Internet. Research and policy challenges in comparative perspective* (1st ed., Vols. 1–26, Vol. 26), Bristol/Chicago: The Policy Press. as cited by E. Vanderhoven, *o.c.*, 224.

3. AT THE LIMITS OF "NOTICE & CONSENT"

3.1 Why notice?

OSN providers provide privacy notices in an **attempt to secure the "informed consent"** of their users. The current approach, whereby the user is forced to accept lengthy privacy notices before being able to access the service, has been subject of increasing criticism.[40] Before discussing these critiques, we must note that privacy notices can do more than just "informing" consent. Notices can fulfill an array of **other functions**, provided those functions are properly understood by all stakeholders involved.[41] If drafted properly, privacy notices can:

a) promote fairness;
b) help to compensate knowledge asymmetries;
c) enable data subjects to contest abusive data practices;
d) have a 'purifying' effect on data controller's actual practices; and
e) enhance the accountability of data controllers.[42]

3.2 Regulatory failure

Notice and consent mechanisms start from the assumption that data subjects can fully understand what will happen if they consent to the processing of their data.[43] In practice, privacy notices are often complex, provider-centred and lack meaningful transparency.[44] Even though they are intended for users, they seem to be drafted by lawyers for lawyers.[45] As a result, OSN users often do not read or do not fully understand this type of legal communication.[46]

From an OSN provider's perspective, there is an economic incentive to collect as much data as possible.[47] Many service providers see privacy notices merely as a

---

[40] For a discussion see B. Van Alsenoy, "D6.1 Legal requirements for privacy-friendly model privacy policies", SPION Project, 30 June 2012, 16, available on www.spion.me. See also House of Commons Science and Technology Committee, "Responsible use of data", Fourth Report of Session 2014-15, 19 November 2014, p. 18 et seq, accessible at http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf

[41] For a comprehensive analysis see R. Calo, 'Against Notice Skepticism in privacy (and elsewhere)', *Notre Dame Law Review* 2012, vol. 87, 1027 et seq.

[42] See B. Van Alsenoy, D6.1 Legal requirements for privacy-friendly model privacy policies", *l.c.*, 7-10.

[43] Article 29 Working Party, "Opinion 15/2011 on the definition of consent", 13 July 2011, 9, 17, available on http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

[44] V. Donoso and V. Verdoodt, "White Paper Social media literacy: Time for an update!", EMSOC Project, 2014, 21, available on www.emsoc.be.

[45] *Idem.*

[46] E. Wauters, V. Donoso and E. Lievens, "Why are Terms of Use so difficult to understand? Reflections on how to optimize transparency for users in Social Networking sites", EuroCPR, Brussels, 24-25 March 2014. See also A. Bechmann (2014). "Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook", *Journal of Media Business Studies,* Vol. 11, Issue 1, 21-38.

[47] P. Lambert, *Social Networking: Law, Rights and Policy*, Clarus Press, 3 April 2014, 107.

compliance burden on which only a minimum amount of effort should be spent.[48] By obtaining consent of their users, they try to avoid any constraints for the future use of the data they collect and shield themselves against potential complaints or legal actions.[49] From a marketing perspective, organisations have an incentive to embellish potentially unpopular processing practices as much as possible. As a result, privacy notices are often characterised by vagueness, obscurity and boilerplate language.[50] Another reason why privacy notices fail their regulatory objective in practice relates to the enforcement and oversight. At the moment, many DPAs only have limited means and resources to enforce data protection laws.[51] As a result, there is no strong push for OSN providers to provide more meaningful transparency.

3.3 Recommendations

Apply a clear distinction, both conceptually and in practice, between 'notice' and 'consent'. [52] Debates regarding the (in)utility of privacy notices often confound two very distinct issues, namely transparency on the one hand, and legitimacy on the other. Lengthy privacy notices generally do not lead to informed consent.[53] This finding does not, however, imply that comprehensive privacy notices are pointless. Comprehensive notices can be instrumental in the evaluation of compliance an organisation's data practices, promote basic fairness of processing (by putting data subjects 'on notice' that their personal data is being processed), and promote general awareness of data subject rights.

Actual "legitimacy" requires substantive justification. Consent should not be employed as a freestanding, "lazy" justification for the processing of personal data.[54] Data processing can only be truly legitimate if it is proportionate and if all the interests of the different actors involved have been taken into account.[55] OSN providers are responsible for ensuring that a fair balance between the privacy interests of individuals

---

[48] P. Van Eecke and M. Truyens, "EU study on the Legal analysis of a Single Market for the Information Society - New rules for a new age?", November 2009, 42.

[49] B. Van Alsenoy, E. Kosta and J. Dumortier, "Privacy notices versus informational self-determination: Minding the gap", *International Review of Law, Computers & Technology* 2013, p. 6.

[50] P. Van Eecke and M. Truyens (eds.), 'The future of online privacy and data protection', *l.c.*, p. 42. See also R. Leenes and E. Kosta, "Taming the cookie monsters with Dutch law – a tale of regulatory failure", *Computer Law & Security Review* 2015, Vol. 31, Issue 2, forthcoming.

[51] R. Leenes and E. Kosta, "Taming the cookie monsters with Dutch law – a tale of regulatory failure", *l.c.*, forthcoming.

[52] B. Van Alsenoy, E. Kosta and J. Dumortier, "Privacy notices versus informational self-determination: Minding the gap", l.c., p. 8 et seq..

[53] R. Leenes and E. Kosta, "Taming the cookie monsters with Dutch law – a tale of regulatory failure", *Computer Law & Security Review* 2015, Vol. 31, Issue 2, forthcoming.

[53] *Idem*.

[54] R. Brownsword, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality', in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), *Reinventing Data Protection*, 2009, Springer, p. 90.

[55] A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy." in S. Gutwirth, Y. Poullet, P. De Hert, C. Terwange and S. Nouwt (eds.), *Reinventing Data Protection?*, Springer, 2009, 73.

and commercial interests of business is maintained at all times. Policymakers and regulators should set clear boundaries for OSN providers and third parties, which will make it easier to determine whether certain processing activities are acceptable or not.[56]

"Requiring" vs. "requesting" information. There is a qualitative difference between information which is necessary for a service to function technically and information which is collected to support a company's business model.[57] For consent to be freely given, individuals should have the ability to give free and specific consent to receiving behavioural advertising *independently* of his access to the social network service.[58]

Explore more effective ways of presenting information.[59] Information can be presented in many different ways (e.g., layering, visualisation or labelling of information), which can facilitate the comprehension of complex legal information. In addition, feedback and awareness tools can promote greater understanding and reflection of individuals.[60] Such tools can show data subjects the possible outcome of a potentially privacy-relevant action in a particular system, and can provide feedback. In turn, individuals can gain greater knowledge of the possible privacy implications of their actions. Visualization tools have been proven useful for users to comprehend their online relationships and access control.[61]

Promote collective transparency mechanisms. Different services have different terms and conditions and different ways of providing information to their consumers. The diversity of information makes it difficult for individual consumers to take informed decisions and understand the differences between service providers. Consumer information should be communicated in comparable and ideally standardized and machine-readable format.[62] This would facilitate the development of more "collective" transparency, e.g. in the form of comparison tools offered by a non-governmental organisation or consumer protection agency.

---

[56] See also B. Van Alsenoy, V. Verdoodt, A. Kuczerawy and G. Acar, D9.6.3 Evaluation of the legal framework applicable to Online Social Networks, January 2015, 30 accessible at www.spion.me.

[57] Based on House of Commons Science and Technology Committee, "Responsible use of data", Fourth Report of Session 2014-15, 19 November 2014, 25, accessible at http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf

[58] Article 29 Data Protection Working Party, "Opinion 15/2011 on the definition of consent", WP187, 25 November 2014, p. 18.

[59] V. Donoso and V. Verdoodt, *o.c.*, 22.

[60] Freebu, a tool that was developed within the SPION Project, is an example of a feedback and awareness tool. See http://www.spion.me/workpackage/feedback-and-awareness-in-online-social-networks.

[61] Lipford, H. R., Besmer, A., & Watson, J. , "Understanding Privacy Settings in Facebook with an Audience View, in *Proceedings of the 1st Conference on Usability, Psychology, and Security*. Berkeley, 2008 USENIX Association, pp. 2:1–2:8 accessible at http://dl.acm.org/citation.cfm?id=1387649.1387651 and S. Egelman, A. Oates and S. Krishnamurthi, "Oops, I Did It Again: Mitigating Repeated Access Control Errors on Facebook", in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2011, New York, ACM pp. 2295–2304.

[62] N. Helberger, "Form matters: Informing consumers effectively", Amsterdam Law School Legal Studies Research Paper No. 2013-71 / Institute for Information Law Research Paper No. 2013-10, 49 accessible at http://ssrn.com/abstract=2354988.

4. DEFAULT MATTERS

4.1 The "power of default"

Many OSN users **do not or rarely modify** default privacy settings.[63] It is therefore important that these settings have pre-selected values that respect the users' privacy.[64] The ideal situation would be for OSN users' privacy to be protected by default, without requiring any actions from them.[65]

When reflecting on the importance of default settings, one should take into account that **several factors** complicate the decision-making process of OSN users. First of all, privacy choices are affected by incomplete information.[66] For instance, many times an information asymmetry between the OSN user and provider exists, as the latter is the only party that is fully aware of the amount of data being collected, the purposes for which this data is being used and which third parties have access.[67] Many privacy decisions do not reflect user expectations because

> "*the complexity of the privacy decision environment leads individuals to arrive at highly imprecise estimates of the likelihood and consequences of adverse events, and altogether ignore privacy threats and modes of protection*".[68]

Even if information would be complete, OSN users' ability to collect and process all this information is limited. The search for relevant information is time- and energy-

---

[63] Article 29 Working Party Opinion 5/2009 on online social networking, 12 June 2009, 7, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf. A distinction should be made however, between privacy settings which enable control over "social privacy" (i.e. which allow users to limit access to "friends" or to "block" certain users) and privacy settings which enable users to control collection and use of data by third parties. For example, Facebook currently offers a (link to) an opt-out for behavioural profiling via cookies. However, this information is only provided under the "Ads" heading rather than the "privacy heading". Individuals configuring their "privacy" settings might thus mistakenly believe that all their data is protected, while in reality they are still being tracked by Facebook across websites. It should also be noted that rarely modifying the default privacy settings is not necessarily an indication of users not caring about their privacy. While users have limited control options in controlling their information flow towards third parties (institutional privacy), they often make use of social strategies for their social privacy (and thus move beyond the available settings in their privacy management).

[64] J. Ausloos, E. Kindt, E. Lievens, P. Valcke and J. Dumortier, "Guidelines for Privacy-Friendly Default Settings", *ICRI Working Paper Series*, 18 February 2013, 4.

[65] Ann Cavoukian, Privacy by Design and the Emerging Personal Data Ecosystem, October 2012, 18, http://privacybydesign.ca/content/uploads/2012/10/pbd-pde.pdf; J. Ausloos, E. Kindt, E. Lievens, P. Valcke and J. Dumortier, "Guidelines for Privacy-Friendly Default Settings", *ICRI Working Paper Series*, 18 February 2013, 24.

[66] A. Acquisti and J. Grossklags, "What Can Behavioral Economics Teach Us About Privacy", presented as Keynote Paper at ETRICS 2006, 1-2.

[67] A. Acquisti and J. Grossklags, "Privacy and Rationality in Individual Decision Making", *IEEE Security & Privacy*, vol3, No 1, January/February 2005, 27; R. Balebako, P.G. Leon, H. Almuhimendi, P.G. Kelly, J. Mugan, A. Acquisti, L.F. Cranor and N. Sadeh, "Nudging Users Towards Privacy on Mobile Devices", *CHI 2011*, May 7 - 12 2011, Vancouver, BC, Canada, 1; I. Adjerid, A. Acquisti, L. Brandimarte, G. Loewenstein, "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency, *Symposium on Usable Privacy and Security (Soups) 2013*, 24-26 July 2013, Newcastle, UK, 2.

[68] A. Acquisti and J. Grossklags, "What Can Behavioral Economics Teach Us About Privacy", presented as Keynote Paper at ETRICS 2006, 3.

consuming and individuals have cognitive limitations, which implies that they can only rationalise to a certain extent about all available data (so-called 'bounded rationality').[69] In other words, OSN users' cognitive constraints causes them to deviate from so-called "rational" privacy decisions.[70]

The nature and design of an OSN platform may also influence privacy decisions. Research has shown that for example Facebook users have problems with accurately estimating their audience on OSNs.[71] The lack of social transparency hinders their understanding of the possible consequences of sharing their personal information on the platform. Consequently, they might share more information than they would otherwise.

4.2 Privacy and data protection by default

The concept of 'Privacy by default' originates from Ann Cavoukian, the former information and Privacy Commissioner of Ontario, Canada, as part of her concept of 'Privacy by design'. According to Cavoukian, **privacy-friendly default settings are one of the seven privacy principles of 'Privacy by design'**.[72] In Europe, this concept has also been promoted by the Council of Europe urging Member States to:

> *"promote best practices for users. This includes default privacy-friendly settings that limit access to contacts selected by users themselves […]."*[73]

More recently, the concept of privacy or data protection by default was taken up by the European Commission in their **proposal for a general Data Protection Regulation** and the European Parliament in its first reading.[74] Once the Regulation comes into force, the principle of data protection by default will oblige the OSN provider to implement

---

[69] M.A. Eisenberg, "The Limits of Cognition and the Limits of Contract", *47(2) Stanford Law Review*, 1995, 214; H.A. Simon, "Models of bounded rationality. Trustme: Anonymous management of trust relationships in decentralize P2P systems", in N. Shahmehri, R.L. Graham & G. Caronni (Eds.), *Peer-to-peer computing*, Washington DC, USA: IEEE Computer Society, 142-149; E. Wauters, E. Lievens, P. Valcke, D1.2.4: A legal analysis of Terms of Use of Social Networking Sites, including a practical legal guide for users: 'Rights & obligations in a social media environment', 19 December 2013, 8, www.emsoc.be.

[70] Y. Wang, P.G. Leon, A. Acquisti, L.F. Cranor, A. Forget and N. Sadeh, "A Field Trial of Privacy Nudges for Facebook", CHI 2014, Toronto, ON, Canada, 1 May 2014, 1.

[71] M.S. Bernstein, E. Bakshy, M. Burke and B. Karrer, "Quantifying the Invisible Audience in Social Networks", *CHI 2013*, April 27–May 2, 2013, Paris, France, 2.

[72] A. Cavoukian, 7 Foundational Principles, 11 December 2014, available on http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/, (date of consultation).

[73] Council of Europe, Recommendation on the protection of human rights with regard to social networking services, 4 April 2012, available on https://wcd.coe.int/ViewDoc.jsp?id=1929453&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383. See also Article 29 Working Party, "Opinion 5/2009 on online social networking", WP163, 12 June 2009, p. 7.

[74] Article 23 Proposal for a General Data Protection Regulation, COM/2012/011 final, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52012PC0011; *Article 23 (2): "In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals and that data subjects are able to control the distribution of their personal data."* See European Parliament legislative resolution of 12 March 2014 on the proposal for a General Data Protection

"privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimisation and purpose limitation."[75]

4.3 Recommendations[76]

Awareness and active choice. Only a limited number of users change their default settings or is even aware that their settings can be tweaked. OSN providers should wait for an affirmative action of the user before sharing his or her information to a broader audience than just "friends" or "connections". In addition, no changes should be made to default settings without the user's affirmative consent. Mere notification of changes is not enough.[77]

Default settings should be simple, logical and easy to find. An overabundance of settings can confuse and even intimidate users.[78] Default settings should not be too overly complex and should focus on the most important questions. Therefore, a simple and logical privacy pane is necessary. OSN providers should aim for a comprehensive "dashboard", making sure that settings can be found in one place without having to click on numerous hyperlinks.[79] At the same time, individuals should also be able to exercise audience controls at the moment of providing information.

Enhance audience visibility. OSN users often underestimate their actual audience when disclosing personal information on their profiles. In this regard, more 'social transparency' is required, for instance by improving audience visibility by default. Social transparency can nudge users into a more cautious approach to online information sharing, as they are forced to think about who is actually watching or listening. For instance, OSN providers could offer an indication of how many people really view a picture or read a statement. Audience visualizations have not been integrated in ONSs so far, even though they are proven useful for users' privacy management.[80]

Regulation, available on http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN.

[75] Recital 61 European Parliament legislative resolution of 12 March 2014 on the proposal for a General Data Protection Regulation.

[76] See J. Ausloos, E. Kindt, E. Lievens, P. Valcke and J. Dumortier, "Guidelines for Privacy-Friendly Default Settings", *ICRI Working Paper Series*, 18 February 2013; V. Verdoodt and B. Van Alsenoy, "Guidelines for Privacy-Friendly Default Settings", SPION Project, December 2014.

[77] V. Verdoodt and B. Van Alsenoy, "Guidelines for Privacy-Friendly Default Settings", SPION Project, December 2014, 12. See also A. Kuczerawy and F. Coudert, "Privacy Settings in Social Networking Sites: Is It Fair?" in S. FischerHübner et al. (Eds.), Privacy and Identity 2010, IFIP AICT 352, 235.

[78] J. Ausloos, E. Kindt, E. Lievens, P. Valcke and J. Dumortier, "Guidelines for Privacy-Friendly Default Settings", *ICRI Working Paper Series*, 18 February 2013, 23.

[79] Of course there is also the possibility of contextual privacy settings, these could be have additional value.

[80] See Lipford, H. R., Besmer, A., & Watson, J. , "Understanding Privacy Settings in Facebook with an Audience View, in *Proceedings of the 1st Conference on Usability, Psychology, and Security*. Berkeley, 2008 USENIX Association, pp. 2:1–2:8 accessible at http://dl.acm.org/citation.cfm?id=1387649.1387651 and S.

Ensure an appropriate level of granularity. OSN providers should offer privacy (default) settings which allow users to freely and specifically consent to any access to their profile's content that is beyond the contacts they selected themselves.[81] Thus, they should allow and stimulate customised settings, whereby users can easily and exactly select a specific audience for their separate posts. Furthermore, OSN users should be able to exercise control over the collection and use of their personal information by the OSN provider and third parties. Finally, OSN providers should enable users to exercise some control over the information about them that is being posted by fellow users.

Consider expiration dates for information shared by OSN users.[82] The information people share on their profiles remains visible unless it is deleted post-by-post. This task costs a lot of effort and is time-consuming. A time setting would allow OSN users to specify for each different post or picture after which period of time it should be automatically deleted or its visibility reduced.

Egelman, A. Oates and S. Krishnamurthi, "Oops, I Did It Again: Mitigating Repeated Access Control Errors on Facebook", in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2011, New York, ACM pp. 2295–2304.

[81] Article 29 Working Party Opinion 5/2009 on online social networking, 12 June 2009, 7, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

[82] Victor Mayer-Schönberger ,"Why we must remember to delete – and forget – in the digital age", The Guardian, 30 June 2011, accessible at http://www.theguardian.com/technology/2011/jun/30/remember-delete-forget-digital-age.

5. UNITED WE STAND

5.1 The power of collective action

In social networks, a large number of individuals can be harmed by the same illegal practice.[83] Data protection laws entitle OSN users to challenge OSN providers in court if they believe their privacy rights have been violated.[84] However, individuals rarely take legal action against an OSN provider. Going to court is expensive and time-consuming, whereas the monetary value of individual claims is low, especially compared to the resources of these major commercial entities. [85]

In 2008, the European Commission published Green Paper on "Consumer Collective Redress", which discussed existing barriers and opened the debate for potential solutions.[86] In 2013, the Commission stressed the importance of "collective redress"[87] as follows

> *"Collective redress facilitates access to justice in particular in cases where the individual damage is so low that potential claimants would not think it worth pursuing an individual claim. It also strengthens the negotiating power of potential claimants and […]."*[88]

Moreover, it recommends all Member States to

> *"have collective redress mechanisms at national level for both injunctive and compensatory relief, which respect the basic principles set out in this Recommendation."*

Collective redress mechanisms should be available horizontally and in different areas where Union law grants certain rights to consumers, including data protection law.[89]

---

[83] European Commission, *Recommendation on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law*, 11 June 2013, available on http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2013_201_R_NS0013.

[84] See also B. Van Alsenoy and V. Verdoodt, "Liability and accountability of actors in social networking sites", SPION D6.3, December 2014, 31 juncto 34.

[85] E. Wauters, E. Lievens and P. Valcke, "Social Networking Sites' Terms of Use: addressing imbalances in the user-provider relationship through ex ante and ex post mechanisms*", JIPITEC* 139, 2014, 140.

[86] European Commission, *Green Paper on Consumer Collective Redress*, 27 November 2011, available on http://ec.europa.eu/consumers/archive/redress_cons/greenpaper_en.pdf.

[87] At the European level, policy makers have always used the term "collective redress", in order to maintain the distinction between the US class actions. See S. Voet, "European Collective Redress: A Status Queastionis", *International Journal of Procedural Law*, vol. 4, 2014, 97-128.

[88] European Commission, *Recommendation on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law*, 11 June 2013, available on http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013H0396&from=EN.

[89] European Commission, *Memo: Frequently Asked Questions: European Commission recommends collective redress principles to Member States*, Strasbourg, 11 June 2013, 2, available on http://europa.eu/rapid/press-release_MEMO-13-530_en.pdf. .

The Recommendation then further elaborates on (non-binding) principles that the Member States should take into account when crafting such mechanisms.[90]

In 2011, the Article 29 Working Party urged the Commission to include collective redress in the proposal for a General Data Protection Regulation. The Working Party believes that if the focus lies too much on the individual exercising his rights, the right to data protection cannot be sufficiently guaranteed.[91] Therefore, the Working Party advocates reducing the burden on claimants, for instance by extending the power to bring a collective action before the courts to the data protection authorities as well as to civil society organisations and associations representing data subject's interests.[92]

5.2 Current mechanisms

Several EU Member States, including Belgium, France, Germany, the Netherlands and Austria already foresee in the possibility of collective action. These mechanisms need to be distinguished from the "class actions" that are common under the US legal system.[93] The latter are rooted in a different legal system with specific features (e.g., punitive damages, contingency fees) which go beyond the European collective redress concept.[94]

In Europe, three different categories of collective redress mechanisms can be distinguished: group actions, representative actions and test procedures.[95] In group actions, the individual claims of a specific category of people can be brought together into one judicial procedure. On the other hand, a representative action can be brought by an organisation, a state body or an individual on behalf of a certain group. In this category of collective redress, the group of individuals represented will not participate

---

[90] S. Voet, "European Collective Redress: A Status Queastionis", *International Journal of Procedural Law*, vol. 4, 2014, 97-128.

[91] Article 29 Data Protection Working Party, *Letter to Commissioner Reding*, 14 January 2011, 2, available on http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_01_14_letter_artwp_vp_reding_commission_communication_approach_dp_en.pdf.

[92] The Commission followed the Working Party and included the possibility for collective redress in its proposal and was amended by the European Parliament. According to Article 73, "*any body, organisation or association which acts in the public interest and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data*." (European Parliament, Legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 12 March 2014, available on http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN)

[93] European Commission, *Press Release: Commission recommends Member States to have collective redress mechanisms in place to ensure effective access to justice*, 11 June 2013, available on http://europa.eu/rapid/press-release_IP-13-524_en.htm.

[94] S. Voet, "European Collective Redress: A Status Queastionis", *International Journal of Procedural Law*, vol. 4, 2014, 97-128.

[95] E. Wauters, E. Lievens and P. Valcke, "Social Networking Sites' Terms of Use: addressing imbalances in the user-provider relationship through ex ante and ex post mechanisms*", JIPITEC* 139, 2014, 140.

in the procedure. Finally, during a test procedure, an individual claim will be tested and serve as a precedent for future cases.[96]

In Belgium, collective redress was only recently introduced into Belgian Code of Economic Law. It is limited in scope, as it is only applicable to consumer-to-business disputes.[97] In order to be admissible, the class action must be based on a breach of contract or on one of the 31 European or Belgian consumer regulations listed.[98] These regulations also relate to privacy, intellectual property, consumer protection, etc., thus a claim based on a privacy infringement would be possible. Secondly, only consumer organisations or authorised non-profit organisations are able to bring a collective action.[99] Finally, the Belgian law requires that the collective action would be more suitable than an individual action.[100]

5.3 Recommendations[101]

Government and consumer organisations should actively promote the use of collective action mechanisms. At the moment, there is an underuse of collective redress by OSN users.[102] This may be attributed to a general lack of awareness regarding the possibility of collective action, for both individual consumers and consumer organisations. Therefore, awareness-raising initiatives should target both individual OSN users and consumer organisations.[103] In this regard, the European Parliament stresses that consumer organisations and the European Consumer Centres Network (ECC-Net) can play a key role in sharing the possibility of collective redress to as many victims of infringements of EU law as possible.[104]

---

[96] *Id.*

[97] Y.S. van der Sype, W. Vandenbussche, I. Samyn and N. Portugaels, "Allen tegen één: Over de rechtsvordering tot collectief herstel en de bescherming van persoonsgegevens op het internet.", *Computerrecht* 2014/180, afl. 6, December 2014, 316.

[98] S. Voet, "Belgium's New Consumer Class Action" in V. Harsagi and C.H. van Rhee (eds), *Multi-Party Redress Mechanisms in Europe: Squeaking Mouses?*, Antwerp, Intersentia, 2014, (forthcoming).

[99] Article XVII.39 Wet van 31 Maart 2014 tot invoeging van titel 2 "Rechtsvordering tot collectief herstel" in boek XVII "Bijzondere rechts procedures" van het Wetboek van economisch recht en houdende invoeging van de definities eigen aan boek XVII in boek I van het Wetboek van economisch recht. *BS* 29 April 2014, 35202-35211. (Act Introducing a Consumer Collective Redress Action in the Code of Economic Law).

[100] The court can take the following elements into account when assessing this requirement: the amount of users participating, individual harm vs. the collective harm, the complexity and judicial efficiency and the legal certainty of the participants. However the value of the individual claims cannot be a decisive factor. See S. Voet, "Belgium's New Consumer Class Action" in V. Harsagi and C.H. van Rhee (eds), *Multi-Party Redress Mechanisms in Europe: Squeaking Mouses?*, Antwerp, Intersentia, 2014, (forthcoming).

[101] The following recommendations have benefitted from the discussions that took place during the "Cultures of Accountability Workshop" in Leuven on 13 November 2014, co-organised by the SPION and PARIS projects.

[102] E. Wauters, E. Lievens and P. Valcke, "Social Networking Sites' Terms of Use: addressing imbalances in the user-provider relationship through ex ante and ex post mechanisms", *JIPITEC* 2014, 142.

[103] *Id.*

[104] European Parliament, Resolution *on 'Towards a Coherent Approach to Collective Redress'*, 2 February 2012, available on http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0021+0+DOC+XML+V0//EN.

Civil society and consumer organisations should receive sufficient resources to undertake collective redress procedures. At the moment, the cost of litigation is too high and many organisations lack the sufficient resources to start a collective action.[105] These organisations need funding in order to overcome the costs threshold of going to court.[106] In addition, data protection authorities require adequate resources to enforce data protection legislation. If DPAs concluded that an entity violated data protection law, this would ease the burden of proof for individuals to claim damages.

Develop standard monetary damages for non-economic harm. Currently, there are no widely accepted objective parameters to estimate the privacy suffered by individuals. Very often, courts award only a symbolic sum (e.g., 1 euro) for moral damages.[107] While there are exceptions[108], the current approach places too great a burden on individuals to demonstrate tangible economic harm.[109]

Enhance coordination and foster cooperation between different organisations advocating consumer rights. At the moment, there is a lack of coordination between different consumer organisations qualified to bring collective action in the different EU Member States.[110] They should cooperate, not only nationally but also on a European level. The European and international organisations that advocate consumer rights, such as BEUC or Consumers International, could play an important role in this respect.[111]

---

[105] E. Wauters, E. Lievens and P. Valcke, "Social Networking Sites' Terms of Use: addressing imbalances in the user-provider relationship through ex ante and ex post mechanisms", *l.c.*, 147.

[106] For instance, the European Consumer Organisation (BEUC) strongly backs the creation of a public fund dedicated to the financing of collective redress brought by consumer organisations. See, BEUC, Litigation funding in relation to the establishment of a European mechanism of collective redress, 2 February 2012, accessible at http://www.beuc.org/publications/2012-00074-01-e.pdf.

[107] E.g., Court of First Instance of Brussels, 15 October 2009, *AM* 2010/2, Luik, 30 June 2010, *AM* 2010/5-6, 551, etc.).

[108] For instance, in a case concerning a Belgian commercial broadcaster who had aired a TV programme showing damaging footage of a person without obtaining this person's consent, the court took into account the audience measurement (702 000 viewers) and estimated the moral damages at 702 000 Belgian francs (17 402 EUR) See Court of First Instance of Brussels (33th Ch.), 19 May 2000, AM 2000/3, 338.

[109] See also the analysis of Y.S. van der Sype, W. Vandenbussche, I. Samyn and N. Portugaels, "Allen tegen één: Over de rechtsvordering tot collectief herstel en de bescherming van persoonsgegevens op het internet.", *Computerrecht* 2014/180, afl. 6, December 2014.

[110] E. Wauters, E. Lievens and P. Valcke, *o.c.*, 147.

[111] *Id.*

6. PETs MAKE GOOD COMPANIONS

6.1 PETs and Privacy by Design

Borking and Blarkom have defined Privacy Enhancing Technologies ("PETs") as

"*a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system*."

Generally speaking, PETs can fulfil one of the following functions:

- to reduce the risk of violating privacy and data protection legislation;
- to minimise the amount of personal data that is being processed; and
- to increase the amount of control of individuals or enhance transparency over the processing of their personal data.[112]

Examples of PETs include encryption[113], anonymisation or pseudonymisation techniques, which can be implemented without hampering the user's social media experience.[114]

The need to implement PETs has been emphasised in the discourse on privacy by design.[115] Privacy by design is a multifaceted concept.[116] In policy and legal documents it is often explained broadly as a general principle, whereas engineers' and system developers' often associate it with the actual implementation of PETs.[117] Ideally, privacy by design is a more comprehensive approach for avoiding risks to privacy; a methodology to incorporate privacy principles in system design, which involves the implementation of PETs.[118] According to the International Conference of Data Protection and Privacy Commissioners, it is a

---

[112] London Economics, "Study on the economic benefits of privacy-enhancing technologies (PET's)", Final Report to the European Commission DG Justice Freedom and Security, July 2010, ix.

[113] An example of an encryption technique developped specifically for OSN is "*Scramble"*: see F. Beato, M. Kohlweiss and K. Wouters, "Scramble! Your Social Network Data", in S. Fischer-Hubner and N. Hopper (Eds.): PETS 2011, LNCS 6794, pp. 211–225, 2011 accessible at https://www.cosic.esat.kuleuven.be/publications/article-2029.pdf.

[114] G. Hornung, "Regulating privacy enhancing technologies. Seizing the opportunity of the future European Data Protection Framework", *Innovation: The European Journal of Social Science Research* 2013, Vol. 26, 182.

[115] However, Privacy by design is broader than implementing PETs, it includes for instance also privacy-friendly default settings. See also D. Klitou, *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century*, Information Technology and Law Series, The Hague, Asser Press, 2014, 270.

[116] European Union Agency for Network and Information Security (ENISA), "Privacy and Data Protection by Design – from policy to engineering", December 2014, 3, available on http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design.

[117] *Idem.* See also S. Gürses, C. Tronsoco and C. Diaz, "Engineering Privacy by Design", accessible at https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf

[118] D. Klitou, *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century*, Information Technology and Law Series, The Hague, Asser Press, 2014, 270.

"*holistic concept that may be applied to operations throughout an organisation, end-to-end including its information technology practices, processes, physical design and networked infrastructure*."[119]

Privacy by design has also found its way into the proposed General data protection Regulation.[120] Article 23 of the proposed Regulation requires data controllers to implement appropriate technical and organisational safeguards. This requirement has to be fulfilled both at the time of determining the purposes and means of the processing and the time of the processing itself. Furthermore, data controllers have to ensure that data protection is embedded within the entire lifecycle of the technology, from the design phase all the way to the final disposal.[121]

6.2 No PETs allowed?

To date, there has been no large-scale adoption of PETs.[122] There are several possible reasons for this. First, many system developers are not yet familiar with privacy principles or privacy-friendly technologies. Most of the time their work merely focuses on the technical aspects and the realisation of functional requirements.[123] In addition, data protection authorities do not have sufficient resources to evaluate the degree of implementation of PETs in todays' ICT landscape.[124]

From the perspective of an OSN provider, there is are generally insufficient incentives to commit to the implementation of PETs. Most of the time these technologies do not offer any direct commercial advantages and OSN providers therefore do not feel inclined to invest in the implementation of PETs. In addition, OSN providers are always careful to avoid any constraints for the future use of the data they collect (e.g., no longer being available to cross-reference user-provided data with data collected from other

[119] 32nd International Conference of Data Protection and Privacy Commissioners, Privacy by design resolution, Jerusalem, Israel, October 2010.
[120] See also privacy by default (supra).
[121] Recital 61, European Parliament, Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). See also Organisation for Economic Co-operation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 2013, 23.
[122] See also London Economics, "Study on the economic benefits of privacy-enhancing technologies (PET's)", Final Report to the European Commission DG Justice Freedom and Security, July 2010, available on http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf and S. Gürses and C. Diaz. "Two tales of privacy in online social networks", *IEEE Security & Privacy* (2013). Vol. 11, Issue 3, 29–37.
[123] European Union Agency for Network and Information Security (ENISA), "Privacy and Data Protection by Design – from policy to engineering", December 2014, 2, available on http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design.
[124] European Union Agency for Network and Information Security (ENISA), *o.c.*, 1-2.

sources).[125] Certain OSN providers have even gone so far as to restrict the use of PETs on their platforms.[126]

6.3 Recommendations

The legal framework should attach greater importance to PETs. The current legal framework places far greater emphasis on the ex-post securing of personal data than on an ex-ante elimination of risk.[127] Instead, law and technology should complement the protection of individuals' rights to privacy and data protection.[128]

Governments should lead by example. By adopting PETs in their own systems and infrastructure, governments can impact future assessments of what reasonably can be expected from data controllers.[129] As a result, the demand of privacy by design will increase, which in turn will stimulate the market for privacy-friendly services.[130]

The research community, policy makers and data protection authorities should enhance PET awareness.[131] Awareness is the first step towards adoption. Research has shown that awareness is far from universal, although some PETs are much better known than others.[132] Efforts should be made to increase awareness among different target groups, including software developers and system providers, policymakers and data controllers.[133]

---

[125] B. Van Alsenoy, E. Lievens, K. Janssen, J. Dumortier, K. Rannenberg, S. Yang, T. Andersson, Q. Abbas, H. Leitold, B. Zwattendorfer, "A Regulatory Framework for INDI Operators", Global Identity Networking of Individuals Project, 2012, 42.

[126] For instance, Facebook recently deleted an application ("Reclaim") that protected photos of Facebook users against commercial exploitation of their pictures. Facebook also deleted any photos protected by the software. See M. Persson, "Facebook maakt korte metten met beschermde foto's", *de Volkskrant.nl*, 25 January 2015, accessible at http://www.volkskrant.nl/tech/facebook-maakt-korte-metten-met-beschermde-fotos~a3837298.

[127] B. Van Alsenoy, E. Lievens, K. Janssen, J. Dumortier, K. Rannenberg, S. Yang, T. Andersson, Q. Abbas, H. Leitold, B. Zwattendorfer, *o.c.*, 43. See also C. Diaz, O. Tene and S. Gürses, "Hero or Villain: The Data Controller in Privacy Law and Technologies", Ohio State Law Journal 2013, Vol. 74, no. 6, p. 923 et seq., accessible at https://www.cosic.esat.kuleuven.be/publications/article-2365.pdf

[128] A. Roßnagel, *Allianz von Medienrecht un Informationstechnik?*, Baden-Baden, Nomos, 2001, as cited by G. Hornung, "Regulating privacy enhancing technologies. Seizing the opportunity of the future European Data Protection Framework", *Innovation: The European Journal of Social Science Research* 2013, Vol. 26, 182.

[129] B. Van Alsenoy, E. Lievens, K. Janssen, J. Dumortier, K. Rannenberg, S. Yang, T. Andersson, Q. Abbas, H. Leitold, B. Zwattendorfer, *o.c.*, 43.

[130] European Union Agency for Network and Information Security (ENISA), *o.c.*, 51.

[131] B. Van Alsenoy, E. Lievens, K. Janssen, J. Dumortier, K. Rannenberg, S. Yang, T. Andersson, Q. Abbas, H. Leitold, B. Zwattendorfer, "A Regulatory Framework for INDI Operators", Global Identity Networking of Individuals Project, 2012, 44.

[132] London Economics, "Study on the economic benefits of privacy-enhancing technologies (PET's)", Final Report to the European Commission DG Justice Freedom and Security, July 2010, available on http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[133] European Union Agency for Network and Information Security (ENISA), "Privacy and Data Protection by Design – from policy to engineering", December 2014, 52, available on http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design.

Increase incentives for PETs adoption.[134] At the moment, there is a lack of incentive for service providers and system manufacturers to develop privacy-friendly and legally compliant services and products.[135] ENISA has recommended several measures to increase the incentive for adopting PETs, such as audit schemes, seals, higher penalties, or taking into account the implementation of PETs when deciding upon penalties for privacy infringements.[136]

Promote further standardisation and recognition of PETs. In order to increase implementation in practice, standardisation bodies need to provide more standards for privacy-friendly features. In addition, other initiatives to promote the recognition of these technologies should be explored, including voluntary accreditation or official endorsements by regulators.[137]

Consider labelling restrictions on the use PETs as an "unfair commercial practice". OSN providers sometimes restrict the adoption of PETs in relation to their services. The Unfair Commercial Practice Directive foresees in a list of commercial practices that are in all circumstances considered unfair and forbidden.[138] One way to safeguard the use of PETs in an OSN environment would be to label restrictions upon the use of PETs as an unfair commercial practice.

PETs are not a "silver bullet". The potential impact of PETs in creating privacy-friendly social networks should not be overestimated. The mere implementation of PETs is not sufficient to protect the privacy of individual OSN users.[139] PETs can still be circumvented, although the level of difficulty depending on the level of sophistication of the PET.[140] For instance, anonymisation techniques are vulnerable, considering the possibility of de-anonymisation through sophisticated data analysis and data mining techniques.[141]

---

[134] European Union Agency for Network and Information Security (ENISA), *o.c.*, 50.
[135] For an analogy with the clean energy market see D. D. Hirsh, "The glass house effect: big data, the new oil, and the power of analogy", *Maine Law Review*, Vol. 66:2, 2014, 392-393. Hirsh argues that the development of PETs will be confronted with the same market failures as the market of clean energy technologies. Following his analogy, governments should directly invest in the development PETs; offer loan programs for private actors developing PETs; allow tax preferences; when purchasing data analytics services, prefer firms that employ PETs.
[136] European Union Agency for Network and Information Security (ENISA), *o.c.*, 51.
[137] B. Van Alsenoy, E. Lievens, K. Janssen, J. Dumortier, K. Rannenberg, S. Yang, T. Andersson, Q. Abbas, H. Leitold, B. Zwattendorfer, *o.c.*, 45.
[138] European Parliament and Council Directive (EC)2005/29 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005] OJ L149/22 (Unfair Commercial Practices Directive), accessible at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0029&from=en.
[139] European Union Agency for Network and Information Security (ENISA*), o.c.*, 1.
[140] D. Klitou, *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century*, Information Technology and Law Series, The Hague, Asser Press, 2014, 270.
[141] D. Klitou, *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century*, Information Technology and Law Series, The Hague, Asser Press, 2014, 270.

7. CONCLUSION

There is no one-size-fits-all solution for mitigating privacy and security concerns in OSN platforms. It is rather a combination of different approaches, which reflect the different roles of the actors in an OSN environment. Throughout our research, five themes emerged from which we elaborated a set of policy recommendations. These recommendations focus on the one hand on providing the means and knowledge to empower users, while on the other hand enhancing the accountability of OSN providers.

- ***Invest in education and awareness.*** More and more children and youngsters are joining OSNs. These platforms provide a lot of opportunities for young people especially in terms of socialisation, access to information and learning. However, it is important to keep in mind that there are challenges related to the use of OSNs. It is crucial that these young OSN users are well informed and aware of the potential risks OSNs may pose. Formal education has an important role to play here, as schools are able to reach most, if not all children.
- ***Move beyond the limits of notice and choice***. Considering the amount of data collected on OSN platforms, it is important that OSN users are properly informed about these processing activities. Feedback and awareness tools can complement ex ante transparency mechanism and promote greater understanding and reflection of individuals. In addition, policymakers and regulators should set clear boundaries for OSN providers and third parties to determine whether certain processing activities are acceptable or not.
- ***Defaults matter***. OSN users are often prevented from taking decisions related to their privacy. Their decision-making process is complicated by several factors, including inter alia audience visibility, cognitive and behavioural constraints, etc. Privacy-friendly default settings can go a long way in protecting privacy and decrease the burden on individuals.
- ***Promote collective redress.*** Individuals find it difficult to enforce their privacy rights and rarely take legal action. Collective redress mechanisms can significantly reduce the burden on individuals and facilitate access to justice. Civil society and consumer organisations should receive sufficient resources to initiate and co-ordinate collective redress procedures.
- ***PETs make good companions.*** Traditional regulatory instruments are unable to cope with the challenges posed by modern data processing. By shifting the focus from ex-post securing of personal data to ex-ante elimination of risk and shaping technology in a privacy-friendly way, the risk of violating privacy and data protection legislation can be reduced significantly.