

UN Office of the United Nations High Commissioner for
Human Rights (OHCHR) Consultation in connection with
General Assembly [Resolution 34/7 “The Right to Privacy
in the Digital Age”](#)

Submitted by:

[Catherine Garcia van Hoogstraten, Lecturer in Data Governance,
Human Rights, Technology & Cybersecurity at The Hague
University of Applied Sciences](#) and [Nicolás E. Díaz-Ferreyra
Research Fellow at User-Centred Social Media Research Training
Group University of Duisburg-Essen](#)¹

6th April, 2018

¹ Garcia van Hoogstraten and Diaz Ferreyra are doing joint inter-disciplinary research at the intersection human rights in the digital age, privacy and risk management with a strong focus on user-centered technologies and public policy.

Executive Summary

Submissions and recommendations cover two main themes in relation to points 6 and 5 of the call for inputs: Undue interferences with the right to privacy in the digital age that may have particular effects for women, as well as children and persons in vulnerable situations or marginalized groups, and approaches to protect those individuals. Furthermore, on the extent that new technologies help promote and protect the right to privacy

We make the following recommendations to OHCHR:

1. The High Commissioner should explicitly recognize that users' *right to be informed* on the risks of sharing personal information in Social Network Sites (SNSs). Scholars have suggested that users who are more aware of the consequences of online interaction are less likely to share private information in SNSs and more likely to protect their privacy. This lack of information modulates the perceived severity of privacy risks in favor of information disclosure and, consequently, in benefit of the service providers.
2. The High Commissioner should reiterate that States owe human rights obligations to all individuals subject to their jurisdiction. Considering the right to privacy as universal right whose enjoyment does not depend on nationality or location.
3. The High Commissioner should emphasized that privacy scandal unleashed by Facebook-Cambridge Analytics in the last days has damaged the trust of people in social media platforms in a severe way. Such events urge developers of media technologies and public policy makers to cooperate on behalf of the users' privacy rights.

4. The High Commissioner should emphasized that policies and regulations on new technologies may need to encompass provisions on infrastructure, trust, security, and skills. Furthermore, a societal impact assessment, addressing risks, consequences of technologies, policies, programs, systems.
5. The High Commissioner should explicitly recognize that in order to engage with the users, there is the need to deploy preventative technologies, which should follow a set of basic design principles, accordingly: a) adaptive, by taking users' privacy attitudes and intentions into account, b) visceral, by bridging the emotional gap between the users and their private digital data and c) supportive, by recommending heuristics (best practices) to overcome potential privacy issues.

Introduction

1. In relation to the undue interferences with the right to privacy in the digital age that may have particular effects for women, as well as children and persons in vulnerable situations or marginalized groups, we wish to share some takeaways of the 2016 United Nations Internet Governance Forum workshop on Decrypting Sextortion². Here we both contributed as facilitators and organizers. First, that if we want to think about policies and regulations minimizing and controlling the impact and scale of online harassment based on non-consensual distribution of sexual images, it is of crucial importance that we need to think of it as socio-tech problem. Thus, as something that is contextually constituted by the interactions of human behaviour, technical interfaces, and social context. Second, the current architecture of internet and social media enable increased forms of exposure. These vulnerabilities leads to scalability, replicability and searchability of the flagged material. Lastly, we proposed and

² [United Nations Internet Governance Forum 2017 workshop on Decrypting Sextortion](#)

Instructional Awareness System³ (IAS), a risk-driven preventative technology which generates a tailored warning message when a regrettable scenario is detected.

2. We submit for your consideration that Social Network Sites (SNSs) are spaces which are not free of privacy risks. One of the main characteristics of this platforms are their information sharing features which allow user-generated content to reach wide and diverse audiences within a few seconds. Whereas the spectrum of shared content is large and varied, it can nevertheless include private and sensitive information. Such content of sensitive nature can derive in unwanted incidents for the users (such as reputation damage, job loss, or harassment) when reaching unintended audiences. Whether consciously or unconsciously, we interact with risky situations in our daily lives. From jaywalking or smoking cigarettes, people evaluate the potential consequences of risky actions on a daily basis. Likewise, risk-awareness strategies⁴ are used every day to inform people about the risks of engaging with certain activities or consuming products or services. However, when it comes to Social Network Sites (SNSs), users are not given much information about the privacy risks of online interaction. Moreover, when users give their consent for data collection and processing (i.e. when they accept the privacy policy), they receive very little (for not saying none) information about such risks. This lack of information modulates the perceived severity of privacy risks in favor of information disclosure and, consequently, in benefit of the service providers.
3. Like privacy policies, information sharing interfaces of SNSs also play an important role in shaping our perceptions of information privacy. Such interfaces are the entry point of user-generated content which,

³ Diaz Ferreyra, N. E., Schawel, J., Heisel, M., and Meske, C.(2016). Addressing Self-disclosure in Social Media:An Instructional Awareness Approach. In *Proceedings of the 2nd ACS/IEEE International Workshop on Online Social Networks Technologies (OSNT)*. ACS/ IEEE. Fang, L. and LeFevre, K. (2010). Privacy wizards for social networking

⁴ N. E. Diaz Ferreyra, R. Meis, and M. Heisel, "Should User-generated Content be a Matter of Privacy Awareness? A position paper," in *Proceedings of the 9th International Conference on Knowledge Management and Information Sharing (KMIS 2017)*, November 2017. *The authors* argue that this is a problem of lack of awareness which is grounded in an emotional detachment between the users and their digital data. In line with this, they discuss preventative technologies for raising awareness and approaches for building a stronger connection between the users and their private information. They encourage the inclusion of awareness mechanisms for providing better insights on the privacy policies of SNSs.

in many cases, contains private information. However, since digital data is intangible, information sharing interfaces of SNSs regulate users' emotional perception and attachment towards their private information. Consequently, privacy policies and sharing interfaces are not succeeding in taking the users' emotional perception of their private data to the visceral⁵ level.

4. The privacy scandal unleashed by Facebook-Cambridge Analytics in the last days has damaged the trust of people in social media platforms in a severe way. Such events urge developers of media technologies and public policy makers to cooperate on behalf of the users' privacy rights. In this work, we strongly encourage users' *right to be informed* on the risks of sharing personal information in SNSs. Scholars have suggested that users who are more aware of the consequences of online interaction are less likely to share private information in SNSs and more likely to protect their privacy. Likewise, they suggest that in order to inspire risk reduction behaviors, risks should be perceived as controllable by the users. In line with this premise (i.e. more information, better decisions), our work takes a closer look into risk communication and management strategies for the development of preventative technologies within the social media ecosystem.
5. We submit for your consideration that in order to engage with the users, there is the need to deploy preventative technologies, which should follow a set of basic design principles⁶, accordingly: a) adaptive, by taking users' privacy attitudes and intentions into account, b) visceral, by bridging the emotional gap between the users and their private digital data and c) supportive, by recommending heuristics (best practices) to overcome potential privacy issues.

CONTACT INFORMATION

Catherine Garcia van Hoogstraten J.D., LL.M., MA

Lecturer in Data Governance, Human Rights, Technology & Cybersecurity

⁵ More on 'Data Visceralization' at Nicolas E. Diaz Ferreyra, Rene Meisy, Maritta Heisel(2017) At Your Own Risk: Shaping Privacy Heuristics for Online Self-disclosure.

⁶ Ibid 5



UNIVERSITÄT
DUISBURG
ESSEN

Open-Minded

Faculty of Public Management, Law and Security - The Hague University of Applied Sciences
C.vanHoogstraten@hhs.nl
Johanna Westerdijkplein 75 , 2521 EN The Hague, The Netherlands

Ing. Nicolás E. Díaz Ferreyra
Research Fellow
User-Centered Social Media Research Training Group
University of Duisburg-Essen
nicolas.diaz-ferreyra@uni-due.de
Room BB 918, Oststrasse 99, 47057 Duisburg, Germany