Inequality in Online Privacy: Direct and Indirect Sociodemographic Effects on Self-Protection

Moritz Büchi[1], Noemi Festic[1], Natascha Just[2] and Michael Latzer[1]

Privacy governance options range from top-down command-and-control regulation at the one end (e.g., Regulation (EU) 2016/679), to bottom-up user self-help at the other. The inability of the state to guarantee full-fledged protection in global online networks in general (Roßnagel, 1997) and the legacy of the conventional liberal privacy paradigm (Bennett & Raab, 2003; Regan, 1995) both account for the more prominent role that user self-help is accorded in this governance mix.

Participating online has become a societal standard and prerequisite for functioning in society by facilitating information seeking or relationship building. Often confronted with "take-it-or-leave-it choices" (Zuiderveen Borgesius et al., 2017), users' complete refusal of data disclosure is not a real option if they wish to profit from the various advantages of using the Internet. Little is known about the wider distribution of privacy protection across societies in general, the extent to which people actively protect their privacy online, and the factors that explain privacy self-help protection on the individual level. Such an understanding is necessary, however, to better comprehend who achieves what level of data protection, and to identify whether there are systematically disadvantaged and vulnerable social groups. In this study, we empirically address the question of how privacy protection behavior at the user level is influenced by sociodemographic attributes, by the amount of peoples' overall Internet use and their Internet skills, as well as by their attitudes towards personal information and past privacy breaches.

Next to the *privacy paradox* (e.g., Barnes, 2006; Norberg et al., 2007), research has also revealed that people are not generally ignorant, but continuously negotiate the kind and amount of personal information they share in order to protect and express themselves against variables that affect their privacy (Young &

[1] University of Zurich, Department of Communication and Media Research, Media Change and Innovation Division
[2] Michigan State University, College of Communication Arts and Sciences, Department of Media and Information

Quan-Haase, 2013). The literature has predominantly revealed privacy concerns and attitudes as well as experienced data breaches as predictors of privacy protection (Baruh et al., 2017). Additionally, general Internet skills have been identified as a key predictor of users' privacy behavior (Büchi et al., 2017).

From its inception, the idea of privacy protection has been predicated on a liberal democratic model, essentially on an individualistic conception of privacy as a special type of "right to be let alone" (Warren & Brandeis, 1890, p. 193). While this individualist privacy paradigm is increasingly being questioned in research with e.g. a recognition of its social value (Regan, 1995; Bennett & Raab, 2003; Nissenbaum, 2010; Solove, 2015), there is still a tendency in policy-making to remain loyal to this legacy. In the EU regulation, there is no provision that accounts for likely disparities among the people it is intended to protect. Such knowledge, however, could assist in detecting inequalities in privacy and data protection and allow adjusting public policies accordingly. To discuss online privacy protection in line with digital inequality scholarship is therefore precisely to rethink this traditional conception of privacy (protection): from a primary emphasis on its importance to individuals to an acknowledgement of its broader importance to societies at large and the likely consequences this entails for policy-making.

As an example, automated assessment methods are increasingly used to determine the "employability" of job candidates. Their social media data is used to calculate their fit for a specific position based on personality type analyses from likes and shares on social media profiles or the assessment of a candidate's network connections to determine their social capital (Madden et al., 2017). It is particularly disadvantaged groups that are most dependent on the decisions made based on their data and who are likely to be unaware of data collection practices (Matzner et al., 2016) or have inadequate skills to manage their own information disclosure on the Internet (Li et al., 2018). Older individuals and women have been shown to have lower levels of technical skills of privacy control. Such disadvantaged groups are then also particularly vulnerable to potential errors or biases embedded in big data-driven, algorithmic systems that make automated decisions (Latzer et al., 2016).

Understanding what factors inhibit privacy protection may provide a basis for improvements in privacy practice and policy. To this end, this paper uniquely conceptualizes online privacy from a digital inequality perspective. It provides nationally representative data from Switzerland (N=970) for an explanatory model of self-help online privacy protection. Using multi-indicator variables (e.g., online privacy protection was measured by the self-reported frequency of changing privacy settings, using fake information online or managing cookies)

and path modeling, the results reveal distinct pathways to online privacy relevant for digital inequality and corresponding policies. Pro-privacy attitudes, experiences of privacy breaches, the amount of Internet use, and general Internet skills led to increased privacy-protective behavior. Amount of use and skills were themselves highly dependent on sociodemographic attributes with younger, male and more educated users reporting higher values. Additionally, lower age and higher education directly predicted higher frequency of privacy protection. Greater age was directly associated with lower self-help privacy protection. Age also had strong indirect negative effects on privacy protection via the amount of Internet use and Internet skills. Low-use and low-skilled older Internet users thus represent a social group particularly vulnerable to experiencing negative Internet use outcomes.

To the extent to which self-help measures of online privacy protection prove effective, the analysis shows that digital inequalities in Internet use carry over to the protection of personal data. Because privacy and control over one's personal data relate to social power and discrimination, inequalities emerging from online behavior on top of long-standing forms of social inequality are problematic. In addition to deeply rooted social inequalities, digital inequalities, in particular in Internet skills, need to be addressed. Privacy breaches are one important way in which Internet use and related variables can negatively affect individuals' well-being and ultimately feed back into life chances and social stratification.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). http://journals.uic.edu/ojs/index.php/fm/article/view/1394/1312

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Bennett, C. J., & Raab, C. D. (2003). *The governance of privacy: Policy instruments in global perspective*. Burlington, VT: Ashgate.

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of Internet skills for online privacy protection. *Information, Communication & Society, 20*(8), 1261–1278. http://dx.doi.org/10.1080/1369118X.2016.1229001

Latzer, M., Hollnbuchner, K., Just, N., & Saurwein, F. (2016). The economics of algorithmic selection on the Internet. In J. Bauer & M. Latzer (Eds.), *Handbook on the economics of the Internet* (pp. 395–425). Cheltenham, Northhampton, UK: Edward Elgar.

Li, X., Chen, W., & Straubhaar, J. (2018). Concerns, skills, and activities: Multilayered privacy issues in disadvantaged urban communities. *International Journal of Communication, 12*, 1269–1290.

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review, 95*(1), 53–125.

Matzner, T., Masur, P. K., Ochs, C., & von Pape, T. (2016). Do-it-yourself data protection – empowerment or burden? *Law, Governance and Technology Series, 24,* 277–305. https://doi.org/10.1007/978-94-017-7376-8_11

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life.* Palo Alto, CA: Stanford University Press.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126. doi:10.1111/j.1745-6606.2006.00070.x

Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy.* Chapel Hill, NC: University of North Carolina Press.

Roßnagel, A. (1997). Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger: Thesen zur Änderung der Staatsaufgaben in einer „civil information society". *Zeitschrift für Rechtspolitik, 30*(1), 26–30.

Solove, D. J. (2015). The meaning and value of privacy. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 71–81). Cambridge, UK: Cambridge University Press. https://doi.org/10.1017/CBO9781107280557

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & Society, 16*(4), 479–500. https://doi.org/10.1080/1369118X.2013.777757

Zuiderveen Borgesius, F. J., Kruikemeier, S., Boerman, S. C., & Helberger, N. (2017). Tracking walls, take-it-or-leave-it choices, the GDPR, and the ePrivacy regulation. *European Data Protection Law Review, 3*(3), 353–368. https://doi.org/10.21552/edpl/2017/3/9