

Does the Internet Deliver?

Eight Values as a Yardstick for the Production, Moderation and Regulation of Public Communication on the Internet

- 0/ Introduction
- 1/ Freedom or Control?
- 2/ Equality or Inequality?
- 3/ Gains or Losses in Diversity?
- 4/ Power Levelling or Power Concentration?
- 5/ Integration or Disintegration of the Public Sphere?
- 6/ High or Low Information Quality?
- 7/ High or Low Discourse Quality?



Security or Vulnerability in the Network?

Security or Vulnerability in the Network?

IN SHORT

The Internet is associated with a number of security risks. Government measures are intended to increase security online, but they can also restrict freedom at the same time. Users themselves can contribute to the protection of privacy, with variation in the subjective assessment of the need for protection. Secret state surveillance requires special legitimation and can easily be abused. The same applies to the manipulative leaking of secret information.

The value “security”¹ refers to protecting against negative effects for individuals and society, the causes of which may be external, but could also be intrinsic to media-brokered, public communication itself. Furthermore, communication itself requires protection.

It is the *pessimistic view* that now prevails when it comes to the question of security or vulnerability on the web. “Security” in the broad sense means the protection of individuals and society from all kinds of negative impacts. A distinction can be drawn between technical, politico-social and cognitive forms of security,² although the concept of security has tended to expand.³ The subjective assessment of security can vary,⁴ e. g. in the protection of privacy, and security expectations are therefore not without controversy.⁵ The public sphere is an area of freedom, which everyone is allowed to enter and in which – especially in the case of the Internet – everyone can communicate largely without restraint. This makes it an area of uncertainty at the same time.⁶ Increasingly, new risks emanating from the Internet are coming to light, e. g. cyber war, cyber-crime, cyber espionage, cyber terrorism,⁷ cyber bullying,⁸ the infringement of personal rights⁹ as well as data-¹⁰ and consumer protection rights.¹¹ There are also risks to the Internet itself, i. e. to the communication and infrastructure contained therein.¹² Providers and users should be able to feel confident that protection is effective and risks are minimised.

This brings us to a much-discussed area: the Internet poses new risks for the *protection of privacy*. Especially in social networks like Facebook, users have to balance their need for privacy with other motivations. If they want to establish or maintain relationships, they must grant personal insights (*self-disclosure*). Privacy is associated with independence, reflection, emotional relief and the possibility of self-revelation.¹³

The thesis of the *privacy paradox* is that there is a contradiction between a great need of Internet users to protect their own privacy, and a high willingness to disclose personal information. This thesis, however, does not stand up to closer empirical scrutiny.¹⁴ Meta-analyses show mixed results.¹⁵ Overall, it is evident that privacy is of great importance to the population, especially informational privacy. The propensity to self-revelation depends on the context: it is significantly higher in personal conversations than online.¹⁶ A growing awareness of the problem could be seen among young people.¹⁷

The main controversy focuses on *government measures* intended to increase security (e. g. in the fight against terrorism), while at the same time restricting freedom, e. g. in the case of surveillance measures whose possibilities have considerably expanded online.¹⁸ A particular problem is the secrecy of such measures, which are thus also exempt from critical scrutiny by the public. Investigative journalism, whistle-blowers and leakers play an important role in uncovering secret surveillance.¹⁹

- 1 Vowe (1999: 395–397, 404). The value of security is contained in McQuail's value of order and cohesion (McQuail 1992).
- 2 Bonß (2011: 44–46). Furthermore, a distinction is drawn between (unpredictable) dangers and (predictable) risks (Bonß 2011: 47–54).
- 3 Daase (2011: 142–148).
- 4 DIVSI/sine (2012: 35–53).
- 5 Daase (2011: 150–153).
- 6 Gusy (2011: 284–286). Vowe (1999: 409) distinguishes between risks emanating from the media and risks for the media themselves. In addition, the media offer the opportunity to increase security, e.g. through rapid citizen communication in crisis situations.
- 7 German Bundestag (2013a).
- 8 mpfs (2016: 49–51).
- 9 German Bundestag (2013b).
- 10 German Bundestag (2013b); Weichert (2013). To the right to be forgotten see DIVSI/iRights. Lab (2015). To Big Data see DIVSI/iRights.Lab (2016).
- 11 German Bundestag (2013c).
- 12 German Bundestag (2013c).
- 13 Trepte et al. (2015: 250).
- 14 Dienlin/Trepte (2015); Heravi/Mubarak/Choo (2018).
- 15 Barth/de Jong (2017); Baruh/Secinti/Cemalcilar (2017); Kokolakis (2017).
- 16 Trepte et al. (2015: 253).
- 17 In 2009, the representative JIM study showed that only 46 percent of 12 to 19-year-olds in Germany had activated the “privacy” options in online communities at that time. In 2010 the share was already 67 percent (mpfs 2010: 44–45), in 2011, 79 percent and in 2012, 87 percent (mpfs 2012: 43–44). The willingness among young people to communicate personal information in their own profile has also declined (mpfs 2010: 44).
- 18 Bauman/Lyon (2013); Penney (2017).
- 19 Garton Ash (2017: 319–347).

Literature

- B** Barth, S., & de Jong, M.D.T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34, 1038–1058.
- Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy: Concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67(1), 26–53.
- Bauman, Z., & Lyon, D. (2013). *Liquid surveillance*. Cambridge: Polity Press.
- Bonß, W. (2011). (Un-)Sicherheit in der Moderne. In P. Zoche, S. Kaufmann, & R. Haverkamp (Eds.), *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken* (pp. 43–69). Bielefeld: transcript.
- D** Daase, C. (2011). Der Wandel der Sicherheitskultur – Ursachen und Folgen des erweiterten Sicherheitsbegriffs. In P. Zoche, S. Kaufmann, & R. Haverkamp (Eds.), *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken* (pp. 139–158). Bielefeld: transcript.
- Deutscher Bundestag (2013a, March 19). *Neunter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft“. Zugang, Struktur und Sicherheit im Netz. Drucksache 17/12541*. Deutscher Bundestag, 17. Wahlperiode.
- Deutscher Bundestag (2013b, March 15). *Fünfter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft“. Datenschutz, Persönlichkeitsrechte. Drucksache 17/8999*. Deutscher Bundestag, 17. Wahlperiode.
- Deutscher Bundestag (2013c, March 14). *Zwölfter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft“. Verbraucherschutz. Drucksache 17/12540*. Deutscher Bundestag, 17. Wahlperiode.
- Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, 45(3), 285–297.
- DIVSI/iRights.Lab (2015). *Das Recht auf Vergessenwerden. Eine Untersuchung des iRights.Lab im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI)*. Hamburg: DIVSI.
- DIVSI/iRights.Lab (2016). *Big Data. Eine Untersuchung des iRights.Lab im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI)*. Hamburg: DIVSI.
- DIVSI/sinus (2012). *DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet. Eine Grundlagenstudie des SINUS-Institutes Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI)*. Hamburg: DIVSI.
- G** Garton Ash, T. (2017). *Free speech: Ten principles for a connected world*. London: Atlantic Books.

Gusy, C. (2011). Der öffentliche Raum – Ein Raum der Freiheit, der (Un-)Sicherheit und des Rechts. In P. Zoche, S. Kaufmann, & R. Haverkamp (Eds.), *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken* (pp. 279–301). Bielefeld: transcript.

H Heravi, A., Mubarak, S., Choo, K.-K.R. (2018). Information privacy in online social networks: Uses and gratification perspective. *Computers in Human Behavior*, 84, 441–459.

K Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134.

M McQuail, D. (1992). *Media performance: Mass communication and the public interest*. London: SAGE.

mpfs (Medienpädagogischer Forschungsverbund Südwest) (2010). *JIM-Studie 2010. Jugend, Information, (Multi-)Media. Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland*. Stuttgart: mpfs.

mpfs (Medienpädagogischer Forschungsverbund Südwest) (2012). *JIM-Studie 2012. Jugend, Information, (Multi-)Media. Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland*. Stuttgart: mpfs.

mpfs (Medienpädagogischer Forschungsverbund Südwest) (2016). *JIM-Studie 2016. Jugend, Information, (Multi-)Media. Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland*. Stuttgart: mpfs.

P Penney, J.W. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review*, 6(2), 1–39.

T Trepte, S., Masur, P.K., Scharnow, M., & Dienlin, T. (2015). Privatheitsbedürfnisse verschiedener Kommunikationstypen on- und offline. Ergebnisse einer repräsentativen Studie zum Umgang mit persönlichen Inhalten. *Media Perspektiven*, (5), 250–257.

V Vowe, G. (1999). Medienpolitik zwischen Freiheit, Gleichheit und Sicherheit. *Publizistik*, 44(4), 395–415.

W Weichert, T. (2013). Big Data. Eine Herausforderung für den Datenschutz. In H. Geiselberger & T. Moorstedt (Eds.), *Big Data. Das neue Versprechen der Allwissenheit* (pp. 131–148). Berlin: Suhrkamp.

The Author

Christoph Neuberger is a full professor for communication science at the Institute for Media and Communication Studies at the Freie Universität Berlin and the executive director of the Weizenbaum Institute for the Networked Society ('The German Internet Institute'), Berlin, which is funded by the Federal Ministry of Education and Research (BMBF). Previously, he was a professor at the Ludwig-Maximilians-Universität München (2011–2019) and the Westfälische Wilhelms-Universität Münster (2002–2011). After his dissertation and habilitation at the Katholische Universität Eichstätt, he held a visiting professorship at the Universität Leipzig (2001/02). He is a regular member of the Bavarian Academy of Sciences and Humanities (BAdW) and the National Academy of Science and Engineering (acatech). He was awarded with several prizes, such as the Schelling Prize of the BAdW for outstanding scientific achievements (2016). His fields of research include the Internet public sphere, online journalism, activities of the press and broadcasting media on the Internet, search engines, social media, journalism theory, media quality, as well as media regulation.

Imprint

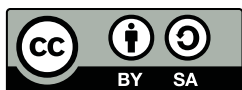
Contact:

Anna Hoffmann
International Media Programmes
European and International Cooperation
T +49 30 / 26 996-3388
anna.hoffmann@kas.de

Dr. Sören Soika
International Media Programmes
European and International Cooperation
T +49 30 / 26 996-3388
soeren.soika@kas.de

Published by:

Konrad-Adenauer-Stiftung e. V. 2020, Berlin
Editor: Philippa Carr (MA), Freelance German into English Translator and Proofreader
Cover page image: © shutterstock/raigvi
Design and typesetting: yellow too Pasiak Horntrich GbR



This publication is published under a Creative Commons license:
"Creative Commons Attribution-Share Alike 4.0 international"
(CC BY-SA 4.0), <https://creativecommons.org/licenses/by-sa/4.0/legalcode>

ISBN 978-3-95721-700-4

www.kas.de