

The Tech Company Dilemma

Ethical Managerial Practice in Dealing with Government Data Requests

Presentation of a PhD Project

1. Introduction

Technology can be instrumental in realizing human rights issues in democratic states and fragile states alike, for instance by enabling freedom of expression or helping to prevent violent conflict through democratic mobilization and exchange. Particularly in the literature on the Arab Spring, the potential of technology as ›liberation technology‹ has been highlighted (cf. Diamond 2015: 3f.). This relates to a broader debate about the availability of tech empowering political and social activism and contributes to the emergence of a new public sphere, as it could be observed during the Hong Kong Umbrella Revolution (cf. Lynch 2011: 305f.; Tsui 2015: 2). At the same time, sceptics have drawn attention to the fact that tech can also become a repression technology (cf. Lynch 2011: 305 f.). For example, new technologies can be used by government authorities for repression of political opponents: for instance, cases of digital government surveillance of political activists were documented in China and Syria (cf. Moss 2018: 267f.; Qiang 2019: 54f.). Technology has been a supporting element in human rights abuses, such as by facilitating government surveillance or silencing opposing political voices. Similar to activists, governments increasingly use the new opportunities offered by the internet for achieving their interests (cf. Lynch 2011: 305f.).

No matter the purpose of the use of data, companies constantly collect rapidly growing amounts of data, in particular personal metrics, for instance via patterns of online behaviour and/or self-tracking devices (cf. Neff/Nafus 2016). This data and societal ›datafication‹ process allows in-depth insights into users' private and professional life, political opinions, social and professional circles, patterns of consumption, and geographic location (cf. Cukier/Mayer-Schoenberger 2013). Also, data profiling of individuals has become easier, cheaper, and widespread: As a consequence, a new information phenomenon emerges (cf. Gasser/Almeida 2017: 59f.). The granularity and scalability of the gathered data can be used for various interests once accessed by a government. During recent years, government requests for user data from internet and telecommunication companies have been documented in elevated numbers – an evident rise that can be seen in transpa-

* Isabel Ebert M.A., Institute for Business Ethics/University of St.Gallen, Girtannerstrasse 8, CH-9010 St.Gallen, Tel.: +41-(0)71-2243103, E-Mail: isabel.ebert@unisg.ch, Fields of Research: Business & Human Rights, Data & Ethics, Internet & Tech Policy.

rency reports from Google (2019) and Telefonica (2018) as well as the Ranking Digital Rights' Corporate Accountability Index (cf. Ranking Digital Rights 2018). Once disclosed, such data can be used by governments to abuse citizens' rights. It should be ensured that disclosure requests for law enforcement are targeted, appropriate in their scope and compliant with applicable legal frameworks. Furthermore, requests could be required, for instance, to be related to criminal cases.

This dilemma raises the question about how responsible business conduct could look like in such a setting, in particular where a company draws the line between legal necessity to comply with a request or corporate responsibility to protect their users' rights. My PhD project will in a first step depict why privacy inhibits such a central role in the human rights framework when dealing with government request for data, and which framework is applied from a global governance perspective (cf. Dingwerth/Pattberg 2006; Keohane/Nye 1977). In a second step, the corporate responsibility to respect human rights from a Business and Human Rights perspective in this setting will be sketched, discussing how this concept relates to government data requests for user data (cf. Ruggie 2007, 2013; Wettstein 2016). Based on expert interviews with senior management of tech companies (both ICT and internet companies), the empirical part of the research analyses how responsible business conduct could emerge when dealing with government requests for data disclosure, applying a sensemaking approach (cf. Maitlis/Christianson 2014; Weick 1988, 1995, 2010; Weick et al. 2005).

This research combines insights from political science and legal scholarship, and follows a Business and Human Rights perspective (cf. Ruggie 2007, 2013), departing from an Integrative Economic Ethics approach (cf. Lorch/Beschorner 2018; Ulrich 2008; Wettstein 2018). In distinction to a Corporate Social Responsibility (CSR) approach (cf. Scherer/Palazzo 2011; Scherer et. al. 2016), Business and Human Rights exerts a rights-based approach, relating to a specific set of values for responsible business conduct, namely human rights (cf. Wettstein 2016, 2018). Human rights here serves as a »targeted reference point for practical tools and initiatives« (Wettstein 2018: 82). From a managerial perspective, it is a major asset that Business and Human Rights offer tools and instruments, such as human rights impact assessments as concrete ways to align human right with the core of the business processes in companies (cf. Wettstein 2016). It is further combined with insights from research in information science: Soghoian (2011) points out the lack of transparency regarding corporate data disclosure practices to governments from an information science perspective.

The corporate responsibility to respect human rights has been laid down in the United Nations Guiding Principles on Business and Human Rights (UNGPs), as adopted by the United Nations Human Rights Council in 2011 (cf. Alston 2006; Clapham 2006; Ruggie 2007, 2013; Wettstein 2015, 2016). The guiding principles are based on three pillars: the state duty to protect human rights, the corporate responsibility to respect human rights and victims' access to effective remedy (cf. UN Human Rights Council 2011). Corporate actors must weigh their decisions on whether and which data to share very carefully in order to protect their users' privacy (cf. Crawford/Schultz 2014). Adding to this, other stakeholder

expectations, such as the ones from customers and investors, become more and more demanding towards companies: Corporate management is under pressure to assure the highest level of privacy protection possible (cf. Flyverbom et al. 2019). Data breaching scandals have led and will continue to lead to tremendous corporate reputation and financial damage (cf. Solon 2016). Consequently, dealing with government requests for data disclosure, and user data specifically, is a precarious issue. Some companies aim at working on paradoxical cases of government requests in a joint manner: The telecommunications industry established the Telecommunications Industry Dialogue (TID) in 2011 to find a common response to threats of human rights abuse implications in operating countries. The TID has merged with the Global Network Initiative (GNI) in 2017, a business network set up in 2008 to uphold human rights both in the telecommunications and the Internet sector (cf. GNI 2019a, 2019b).

Slight progress has been made: Companies such as MTN are complimented upon their human rights policies by civil society (cf. AccessNow 2014), demonstrating a rights-based approach, and companies such as Telefonica increasingly step up on their transparency standards (cf. AccessNow 2017). Yet, the track record regarding data disclosure requests and respecting privacy remains mixed and non-transparent in nature (cf. Soghoian 2011). The above reports also demonstrate that government requests for data disclosure, especially user data, are by no means limited to authoritarian states or states where violent conflict is imminent or manifest: These requests are widespread in Western/OECD-states, especially under the rhetoric of preventing terrorism (cf. Boghosian 2012). However, the potential consequences of these requests in authoritarian states and conflict zones can have much more severe consequences for affected individuals, such as the arrests and/or detentions of opposition members, and/or violent attacks (cf. Flyverbom et al. 2019).

Companies do have a variety of reactions at choice when responding to data requests. Ultimately, their choice of reaction will determine the ›degree‹ of responsible business conduct they can exert. Understanding sensemaking of tech companies in these dilemma situations is critical to analyse opportunities for ethical behaviour. Companies have started to identify initial ways to work jointly on these challenges, yet detailed public information and practice-oriented guidance about individual company behaviour and precise case handling is lacking.

2. Privacy as a Gateway in the Corporate-Government Complex

An intrusion into the private sphere of an individual lays bare data that business models in the data economy use, particularly in data extraction business models. Hence, upholding privacy can be seen as the gateway for human rights protection in the data economy. The right to privacy is a cornerstone in the discussion about ethics in the digital sphere, as a growing number of rights is influenced by digital contexts (cf. Reventlow 2019). It is important to highlight that privacy is not the only issue to be addressed from a human rights perspective in the light of data

disclosure requests. Yet, privacy serves as an entry point for potential infringements of other human rights. Privacy underpins other rights, such as rights that are not individual like freedom of association and assembly (cf. Bernal 2016: 252).

Privacy issues related to the fast spread of information technology have received increasing attention during the last few years. The right to privacy has been recognized as part of the Universal Declaration of Human Rights and in the International Covenant on Civil and Political Rights (1966). Yet, challenges for realizing this human right have changed over time (cf. UN Human Rights Council 2016). The United Nations appointed a Special Rapporteur on the right to privacy in 2015 (cf. *ibid.*: 3). He defines privacy as an ›enabling right‹ closely linked to other rights such as the freedom of expression and freedom of access to information (cf. *ibid.*: 9). The corporate responsibility to respect and ideally promote human rights has been laid down in the United Nations Guiding Principles on Business and Human Rights (UNGPs), as adopted by the United Nations Human Rights Council in 2011 (cf. Clapham 2006; Ruggie 2007).

Information and communication technologies have been discussed as an ambivalent phenomenon in political science and legal studies: Along with the narrative of technology as both a liberation technology as well as a repression technology (cf. Diamond 2015; Lynch 2011), and the intrusive effects of new technologies on privacy (cf. Boyd/Crawford 2012; Cohen 2016; Gasser/Almeida 2017; Zuboff 2015, 2019).

3. The Governance Gap: Government Data Request to the Private Sector

Transnational data flows challenge accountability and responsibility laid down in an international framework which are predominantly based on national jurisdictions. This results in a governance gap regarding the state duty to protect human rights in the essentially transnational data economy with regard to privacy. As a result, privacy protection finds itself in a weak position, especially under limited rule of law. In many cases, ethical company behaviour becomes crucial to upholding privacy. Consequently, companies find themselves in a dilemma situation when confronted with government requests for user data, in particular in trans-border cases.

Governments request data from companies within the same jurisdictions as the one an affected company might be headquartered in, mostly nation state, as well as across jurisdictions. A company might be headquartered in the country of which the authority is requesting the data or a company might be headquartered outside of the jurisdictions of the requesting government authority. Some companies publicly differentiate between ›law enforcement requests‹, as legal demands for customer data from law enforcement agencies, and ›requests for customer data from governments, such as Microsoft (2019). Nevertheless, this difference in definition appears solely cosmetic in nature, as for example Microsoft (*ibid.*) ›follows the same principles for responding to government requests for customer

data« as for responding to law enforcement requests. Hence, the differentiation appears to be artificial in terms of the corporate reaction at choice.

In terms of procedural requirements, many companies state that the request must be made in written and be compliant with local law in quite general terms (cf. Google 2019b; Microsoft 2019; Orange 2016, 2017; Telia 2018; Twitter 2019). Yet it remains challenging for the companies to weigh between the compliance with local law and how this local law might stand in conflict with international law or human rights responsibilities of a company. There is an extensive back and forth about how to regulate data exchanges of corporate data between states. Data exchanges of user data from a company headquartered in the Global North but operating in the Global South or vice versa, might lead to struggles between conflicting definitions of privacy. Keohane and Nye (1977) postulated that the decline of military force as a policy tool and the increase of interdependence, mostly in economic terms, should increase the probability of cooperation among states, yet in the case of data exchanges this remains a complicated undertaking due to conflicting norms, in particular about issues such as human rights, and hence privacy. From a global governance perspective (cf. Dingwerth/Pattberg 2006; Keohane/Nye 1977), this creates ultimately a governance gap for the protection of privacy, partly due to the tension between the interpretation of human rights and state sovereignty over the duty to protect human rights.

4. A Business and Human Rights Perspective on Government Data Requests

Even though government access requests for user data are often discussed from a legal angle, there are reasons why the purely legal discourse in this context is not able to cover privacy issues emerging from a business and human rights perspective. Firstly, legal processes might not serve as the right avenue to address ethical issues arising from privacy across borders. The judgement of one national court might stand in contrast with the judgment of a court in another country. It could be rather seen as an issue that needs to be addressed under a multinational policy making angle to develop a standard for corporate behaviour in line with the UNGPs. Secondly, the leverage that governments can exert in many host or home states on companies, sometimes with the use of force, renders the legal process quite weak (cf. Weber 1978). If staff is threatened or data servers are seized when a company does not comply with a data disclosure request, a cross-border legal processes will be doomed to be ineffective. Hence, a more practice-oriented angle might be necessary to deal with data disclosure requests from the perspective of a corporate manager (or: responsible leader?) who finds oneself in a dilemma situation of conflicting laws and interests.

The majority of data-related requests from governments to tech companies that might infringe privacy or freedom of expression are either to intercept communication traffic or to block it (cf. Tuppen 2016). In either case this can be targeting an individual or a specific website, or also extend to mass action across a whole network, e.g. network-shut downs (cf. *ibid*). Data disclosure requests by govern-

ments focus on the first dimension, the data disclosure requests by government authorities that ask for handover of data obtained and/or collected by companies. We differentiate between two types in the interception dimension for telecommunications companies, as they are used by the telecommunication industry (e.g. cf. Orange 2016) and cyber policy scholars: a) interceptions are requests made by governments or other public authorities, including requisition orders and administrative requests requiring the disclosure of the content of calls, in cyber policy called ›traditional surveillance‹; b) user data that can contain call details (traffic data, including sender, destination, frequency, duration, etc.), customer identification data (first and last names, address, date of birth, etc.), geolocation (relays or GPS coordinates), invoicing and payment information, in cyber policy called ›new surveillance‹ (cf. Bernal 2016). My PhD research focusses on the data types defined under b), which will from now on be referred to either as ›user data‹ or ›meta data‹.

It is noteworthy that meta data can be just as revealing as content data due to the use of smartphones and similar technologies providing insightful data, among others, about geolocation, biometrics including facial recognition and/or fingerprints, and permitting advanced levels of aggregation and analysis (cf. Bernal 2016; Neff/Nafus, 2016). Hence the ›new‹ surveillance by meta data differs in quality and quantity from ›traditional‹ surveillance or interception of communications (cf. Bernal 2016: 246f.).

The data that governmental actors aim to obtain when issuing requests to companies stems from a large, constantly increasing data pool under the possession of the private sector, both data about users, yet increasingly also data collected inside companies about their very own employees (cf. Flyverbom et al. 2019). In particular web browsing data can be used to get insight about intimate, personal information, more than it might be obvious on the first sight: visiting certain websites, searching for specific terms, clicking on particular links, downloading various documents but also the length and frequency of website visits combined with the kind of device used for these purposes (cf. Bernal 2016). Through mathematical profiling, mostly based on correlations by comparative use of extensive amounts of data, the data can reveal personal habits, preferences and tastes and serve as predictor for sexual preferences, political beliefs and religion (cf. Deibert 2019; Neff/Nafus 2016; Zuboff 2019).

In line with the UNGPs, the duty to protect human rights lies with the government as formulated under pillar one (cf. Ruggie 2013). Yet, as described in pillar two, tech companies have the responsibility to respect human rights: Pillar two requires a company to carry out human rights due diligence throughout their operations, as a continuous risk management process to identify, prevent, mitigate and be accountable for addressing its corporate human rights impacts (cf. *ibid.*). As a consequence, tech companies perceive an increased awareness of the risk to become complicit in potential governmental human rights abuses, such as infringements of privacy (cf. MacKinnon 2007; Samway 2016). The accelerating effects of datafication driven forward by new mechanisms for data gathering and interpretation as well as the rise of artificial intelligence push deep into society and

business (cf. Bamberger 2018; Krogh 2018). Finer levels of granularity and scalability of information transform artefacts of social life into data to generate new forms of value (cf. Cukier /Mayer-Schoenberger 2013). This influences how organizations are run. Datafication does not only apply to simple, rather easily-to-automate tasks at the workplace – it might affect ›thinking‹ and knowledge management within organizations (cf. Phan et al. 2017).

Therefore, human rights and in particular respecting privacy, play an increasingly vital role in setting boundaries to deter the data economy from entering full swing »surveillance capitalism« (Zuboff 2015: 75). Due to the global nature of the data economy, this phenomenon is not limited by sector-specific boundaries, national borders or national jurisdictions. Instead, the data processing economy is built on the use of new technologies that enable transnational data flows and are applied in a wide range of interconnected sectors ranging from health care, insurance, construction or food, to private security or services. Hence data collected in all these sectors can be the potential object of a government data disclosure request and tech companies can be seen as only the tip of the iceberg, yet currently any detailed insight into how responsible business conduct can be established in such contexts is lacking and it can be assumed that the tech sector is the most progressed in terms of practice due to confrontation with such data requests from government authorities over a number of years.

5. Making Sense of Government Data Requests

Dealing with data disclosure requests in the age of decentralization in internet governance is an emerging field of practice. Hence, it requires a qualitative research design to better understand the dynamics at hand (cf. Brady/Collier 2010; Strauss 1987). The research should grasp in-depth information and nuanced data on company context, meanings and processes. As sketched before, the field is characterized by little empirical knowledge from a scholarly perspective, hence new themes and directions can emerge inductively (cf. Morse/Mitcham 2002; Strauss 1987). Consequently, the methodological framing of a sensemaking approach (cf. Maitlis/Christianson 2014; Weick 1988, 1995, 2010; Weick et al. 2005) appears as a good fit: Sensemaking occurs in organization when members confront events, issues, and actions that are to a certain extent surprising and confusing (cf. Maitlis/Christianson 2014: 64). This research proposal follows the need expressed by Maitlis and Christianson for more research on the influence of macrosocial structures on sensemaking in organizations, looking at »the social, cultural, economic and political forces that shape what groups will notice, how they can act, with whom they interact, and the kinds of environments that can be collectively enacted« (ibid.: 98). This research gap forms an ideal connection to the research aim of analysing how companies react to data disclosure requests from governments. Obara and Peattie (2018) are among the first to apply the sensemaking approach in the field of Business and Human Rights. The two scholars emphasize that Business and Human Rights scholars have developed a rationale

for business responsibilities towards human rights, yet this rational tends to remain mostly theoretical and normative, with little insight into how companies actually make sense of and use human rights inside the company (cf. *ibid.*: 781). Adding to this, the sensemaking approach allows to make more visible how the Business and Human Rights debate impacts companies' internal dynamics, than solely relying on external documents such as published company policies, reports or impact assessments (cf. *ibid.*: 782). Sensemaking precedes decision-making and follows it through providing questions and answers in a social constructing process (cf. Maitlis 2005; Obara/Peattie, 2018).

Corporate sensemaking about data disclosure requests

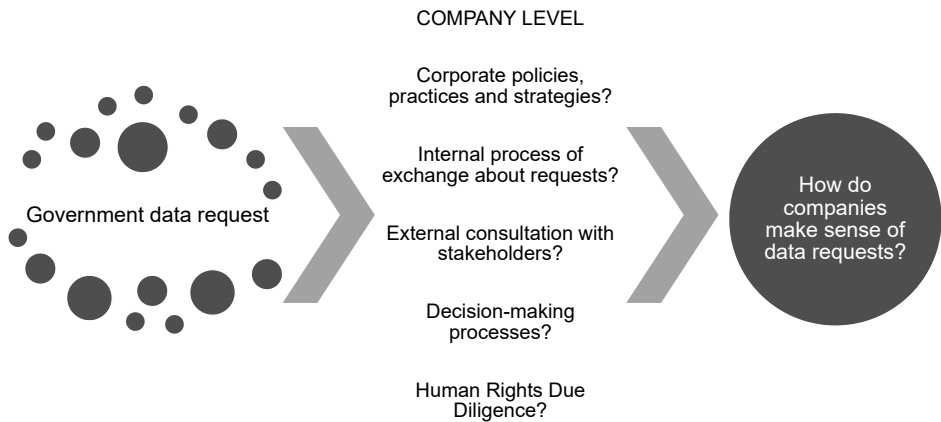


Figure 1: Researching Sensemaking inside Companies about Government Data Requests (Source: own illustration)

The corporate sensemaking about data disclosure requests will be researched based on twenty expert interviews with telecommunication and internet companies. The interviews were chosen to be semi-structured interviews to allow to detect and capture the views and experiences of corporate representatives and through them ideally also the ›social world‹ of the corporate setting, such as adopted formal meaning inside the company and the pre-written processes involved (cf. Obara/Peattie 2018: 784).

6. Outlook

First insights from the expert interviews show that telecommunications companies and internet companies react quite differently when confronted with government data disclosure requests. Telecommunications companies rely on a cooperative relationship with governmental actors to keep their government operating license, and these companies have usually made considerable investments in the

countries they are operating in, such as in personnel and facilities or infrastructure. Internet companies such as Google are less exposed to sanctions by the governments as the headquarter and majority of investments in staff and infrastructure tends to be located outside of a conflict or post-conflict states – mainly in the US or Western Europe. Also, access to the services is usually established through the internet. Internet companies do not have to apply for a license to operate, at the same time governments worldwide increasingly try to regulate internet companies' conduct online. One telecommunications interviewee, for instance, has highlighted the challenges of operating in countries when governments pressured the company to disclose user information during social uprisings, such as in Egypt and Tunisia. The local workforce is more exposed to violent threats and intimidation. Infrastructure can be confiscated or handed over into the property of a competitor who enjoys the local government's support. Yet, the relationship between telecommunications and internet companies is at the same time also of an inter-dependent nature: As telecommunication companies usually act as the internet service providers, they are the intermediary for data transfers to internet companies, such as platforms (cf. Deibert 2008; Lichtman/Posner 2006). Hence, traffic data of internet companies could be intercepted from the internet service provider.

References

- AccessNow* (2014): Access Welcomes MTN Human Rights Policy. Link: <https://www.accessnow.org/access-welcomes-mtn-human-rights-policy/> (last access on June 11, 2019).
- AccessNow* (2017): Telefonica Opens Up as Transparency Standards Improve. Link: <https://www.accessnow.org/telefonica-opens-transparency-standards-improve> (last access on June 11, 2019).
- Alston, P.* (2006): Non State Actors and Human Rights, Oxford: Oxford University Press.
- Bamberger, P. A.* (2018): AMD – Clarifying What We Are About and Where We Are Going, in: Academy of Management Discoveries, Vol. 4/No. 1, 1–10.
- Bernal, P.* (2016): Data Gathering, Surveillance and Human Rights: Recasting the Debate, in: Journal of Cyber Policy, Vol. 1/No. 2, 243–264.
- Boghosian, H.* (2013): The Business of Surveillance, in: Human Rights, Vol. 39/No. 3, 2–5, 23.
- Boyd, D./Crawford, K.* (2012): Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon, in: Information, Communication & Society, Vol. 15/No. 5, 662–679.
- Brady, H. E./Collier, D.* (2010): Rethinking Social Inquiry: Diverse Tools, Shared Standards, Lanham: Rowman & Littlefield Publishers.
- Clapham, A.* (2006): Human Rights Obligations of Non-State Actors, Oxford: Oxford University Press.
- Cohen, J. E.* (2016): The Surveillance-Innovation Complex: The Irony of the Participatory Turn, in: Barney, D./Coleman, G./Ross, C./Sterne, J./Tembeck, T. (Eds.): The Participatory Condition in the Digital Age, Minneapolis: University of Minnesota Press, 207–226.
- Crawford, K./Schultz, J.* (2014): Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, in: Boston Colloge Law Revu, Vol. 55/No. 1, 93–128.
- Cukier, K./Mayer-Schoenberger, V.* (2013): The Rise of Big Data: How It's Changing the Way We Think about the World, in: Foreign Affairs, Vol. 92/No. 3, 27–40.

- Deibert, R. J.* (2008): The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace, in: Chadwick, N./Howard, P. N. (Eds.): Routledge Handbook of Internet Politics, London: Routledge, 339–352.
- Deibert, R. J.* (2019): The Road to Digital Unfreedom: Three Painful Truths About Social Media, in: Journal of Democracy, Vol. 30/No. 1, 25–39.
- Diamond, L.* (2015): Liberation Technology, in: Diamond, L./Plattner, M. F. (Eds.): Liberation Technology – Social Media and the Struggle for Democracy, Baltimore: The John Hopkins University Press, 3–17.
- Dingwerth, K./Pattberg, P.* (2006): Global Governance as a Perspective on World Politics, in: Global Governance, Vol. 12/No. 2, 185–203.
- Flyverbom, M./Deibert, R./Matten, D.* (2019): The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business, in: Business & Society, Vol. 58/No. 1, 3–19.
- Gasser, U./Almeida, V. A.* (2017): A Layered Model for AI Governance, in: IEEE Internet Computing, Vol. 21/No. 6, 58–62.
- GNI* (2019a): Principles on Freedom of Expression and Privacy. Link: <https://globalnetworkinitiative.org/wp-content/uploads/2018/04/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf> (last access on June 11, 2019).
- GNI* (2019b): Implementation guidelines. Link: <https://globalnetworkinitiative.org/implementation-guidelines/> (last access on June 11, 2019).
- Google* (2019): Legal process for user data requests. Link: <https://support.google.com/transparencyreport/answer/7381738?hl=en> (last access on June 11, 2019).
- Keohane, R. O./Nye, J. S.* (1977): Power and Interdependence, Boston: Longman.
- Krogh, G. von* (2018): Artificial Intelligence in Organizations: New Opportunities for Phenomenon-Based theorizing, in: Academy of Management Discoveries, Vol. 4/No. 4, 404–409.
- Lichtman, D./Posner, E. A.* (2006): Holding Internet Service Providers Accountable, Supreme Court Economic Review, Vol. 14/No. 221.
- Lorch, A./Beschorner, T.* (2018): Integrative Economic Ethics: Concept and Critique, in: Heath, E./Byron, K./Marcoux, A. (Eds.): The Routledge Companion to Business Ethics, London: Routledge, 204–219.
- Lynch, M.* (2011): After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State, in: Perspectives on Politics, Vol. 9/No. 2, 301–310.
- MacKinnon, R.* (2007): Shi Tao, Yahoo!, and the Lessons for Corporate Social Responsibility. Link: <http://rconversation.blogs.com/YahooShiTaoLessons.pdf> (last access on June 11, 2019).
- Maitlis, S.* (2005): The Social Processes of Organizational Sensemaking, in: Academy of Management Journal, Vol. 48/No. 1, 21–49.
- Maitlis, S./Christianson, M.* (2014): Sensemaking in Organizations: Taking Stock and Moving Forward, in: Academy of Management Annals, Vol. 8/No. 1, 57–125.
- Microsoft* (2019): Law Enforcement Requests Report. Link: <https://www.microsoft.com/en-us/corporate-responsibility/lerr> (last access on June 11, 2019).
- Morse, J. M./Mitcham, C.* (2002): Exploring Qualitatively-Derived Concepts: Inductive – Deductive Pitfalls, in: International Journal of Qualitative Methods, Vol. 1/No. 4, 28–35.
- Moss, D. M.* (2018): The Ties That Bind: Internet Communication Technologies, Networked Authoritarianism, and ›Voice‹ in the Syrian Diaspora, in: Globalizations, Vol. 15/No. 2, 265–282.
- Neff, G./Nafus, D.* (2016): Self-tracking, Cambridge: MIT Press.
- Orange* (2016): Orange Transparency Report on Freedom of Expression and Privacy Protection. Link: https://www.orange.com/en/content/download/43262/1315009/version/2/file/2017%20RAPPORT%20DE%20TRANSPARENCE_20.6.2017_final_eng.pdf (last access on June 11, 2019).

- Orange* (2017): Respecting Human Rights. Link: <https://www.orange.com/en/Human-Inside/Corporate-responsibility/Our-commitment/Folder/Respecting-human-rights> (last access on June 11, 2019).
- Obara, L. J./Peattie, K.* (2018): Bridging the Great Divide? Making Sense of the Human Rights-CSR Relationship in UK Multinational Companies, in: *Journal of World Business*, Vol. 53/No. 6, 781–793.
- Phan, P./Wright, M./Lee, S.-H.* (2017): Of Robots, Artificial Intelligence, and Work, in: *Academy of Management Perspectives*, Vol. 31/No. 4, 253–255.
- Qiang, X.* (2019): The Road to Digital Unfreedom: President Xi's Surveillance State, in: *Journal of Democracy*, Vol. 30/No. 1, 53–67.
- Ranking Digital Rights* (2018): Ranking Digital Rights Index 2018. Link: <https://rankingdigitalrights.org/index2018/> (last access on June 12, 2019).
- Reventlow, N. J.* (2019): Digital Rights Are *All* Human Rights, Not Just Civil and Political. Link: <https://medium.com/berkman-klein-center/digital-rights-are-all-human-rights-not-just-civil-and-political-daf1f1713f7a> (last access on June 12, 2019).
- Ruggie, J. G.* (2007): Business and Human Rights: The Evolving International Agenda, in: *American Journal of International Law*, Vol. 101/No. 4, 819–840.
- Ruggie, J. G.* (2013): *Just Business: Multinational Corporations and Human Rights*, New York: W.W. Norton & Company.
- Samway, M.* (2016): The Global Network Initiative: How Can Companies in the Information and Communications Technology Industry Respect Human Rights, in: *Baumann-Pauly, D./Nolan, J.* (Eds.): *Business and Human Rights: From Principles to Practice*, New York: Routledge, 136–146.
- Scherer, A. G./Palazzo, G.* (2011): The New Political Role of Business in a Globalized World: A Review of a New Perspective on CSR and Its Implications for the Firm, Governance, and Democracy, in: *Journal of Management Studies*, Vol. 48/No. 4, 899–931.
- Scherer, A. G./Rasche, A./Palazzo, G./Spicer, A.* (2016): Managing for Political Corporate Social Responsibility: New Challenges and Directions for PCSR 2.0, in: *Journal of Management Studies*, Vol. 53/No. 3, 273–298.
- Soghoian, C.* (2011): An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government, in: *Minnesota Journal of Law, Science & Technology*, Vol. 12/No. 1, 191–237.
- Solon, O.* (2016): 2016: The Year Facebook Became the Bad Guy, in: *TheGuardian*. Link: <https://www.theguardian.com/technology/2016/dec/12/facebook-2016-problems-fake-news-censorship> (last access on June 12, 2019).
- Strauss, A. L.* (1987): *Qualitative Analysis for Social Scientists*, New York: Cambridge University Press.
- Telefonica* (2018): Report on Transparency in Communications. Link: https://www.telefonica.com/documents/1258915/129595464/Telefonica_Transparencia_ENG_interactive.pdf/7b0a3737-e3be-4dd4-8d60-f47643b52a48 (last access on June 12, 2019).
- Telia* (2018): Law Enforcement Disclosure Report. Link: <https://www.teliacompany.com/en/sustainability/reporting/law-enforcement-disclosure-report/> (last access on June 12, 2019).
- Tsui, L.* (2015): The Coming Colonization of Hong Kong Cyberspace: Government Responses to the Use of New Technologies by the Umbrella Movement, in: *Chinese Journal of Communication*, Vol. 8/No. 4, 1–9.
- Tuppen, C.* (2016): Opening the Lines. A Call for Transparency from Governments and Telecommunications Companies, in: *Global Network Initiative*. Link: https://globalnetworkinitiative.org/wp-content/uploads/2016/10/GNI_OpeningtheLines.pdf (last access on June 12, 2019).
- Twitter* (2019): Guidelines for Law Enforcement. Link: <https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support> (last access on June 12, 2019).
- Ulrich, P.* (2008): *Integrative Economic Ethics: Foundations of a Civilized Market Economy*, Cambridge: Cambridge University Press.

- UN Human Rights Council (2016): Report of the Special Rapporteur on the Right to Privacy (A/HRC/31/64).
- UN Human Rights Office of the High Commissioner (2011): Guiding Principles on Business and Human Rights. Implementing the United Nations »Protect, Respect and Remedy« Framework (HR/PUB/11/04).
- Weber, M. (1978): *Economy and Society: An Outline of Interpretive Sociology*, Berkeley: University of California Press.
- Weick, K. E. (1988): Enacted Sensemaking in Crisis Situations [1], in: *Journal of management studies*, Vol. 25/No. 4, 305–317.
- Weick, K. E. (1995): *Sensemaking in Organizations*, Thousand Oaks: Sage.
- Weick, K. E. (2010): Reflections on Enacted Sensemaking in the Bhopal Disaster, in: *Journal of Management Studies*, Vol. 47/No. 3, 537–550.
- Weick, K. E./Sutcliffe, K. M./Obstfeld, D. (2005): Organizing and the Process of Sensemaking, in: *Organization Science*, Vol. 16/No. 4, 409–421.
- Wettstein, F. (2015): Normativity, Ethics, and the UN Guiding Principles on Business and Human Rights: A Critical Assessment, in: *Journal of Human Rights*, Vol. 14/No. 2, 162–182.
- Wettstein, F. (2016): From Side Show to Main Act: Can Business and Human Rights Save Corporate Responsibility, in: Baumann-Pauly, D./Nolan, J. (Eds.): *Business and Human Rights: From Principles to Practice*, New York: Routledge, 77–87.
- Wettstein, F. (2018): Social Responsibility, in: Heath, E./Byron, K./Marcoux, A. (Eds.): *The Routledge Companion to Business Ethics*, London: Routledge, 167–183.
- Zuboff, S. (2015): Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, in: *Journal of Information Technology*, Vol. 30/No. 1, 75–89.
- Zuboff, S. (2019): *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power*, New York: Public Affairs.