

The Tech Company Dilemma – Navigating Government Requests for User Data

DISSERTATION
of the University of St.Gallen,
School of Management,
Economics, Law, Social Sciences,
International Affairs and Computer Science,
to obtain the title of
Doctor of Philosophy in Organizational Studies and Cultural Theory

submitted by

Isabel Laura Ebert

from

Germany

Approved on the application of

Prof. Dr. Florian Wettstein

and

Prof. Dr. Gina Neff

Dissertation no. 5042

Digitaldruckhaus Konstanz 2021

The University of St.Gallen, School of Management, Economics, Law, Social Sciences, International Affairs and Computer Science, hereby consents to the printing of the present dissertation, without hereby expressing any opinion on the views herein expressed.

St.Gallen, 20 October 2020

The President:

Prof. Dr. Bernhard Ehrenzeller

ACKNOWLEDGEMENTS	5
ABSTRACT	6
SUMMARY	7
SUMMARY IN GERMAN / ZUSAMMENFASSUNG	8
LIST OF ABBREVIATIONS	9
LIST OF FIGURES	10
LIST OF TABLES	11
I. INTRODUCTION	12
II. OPENING BLACK BOXES IN THE DATA ECONOMY AS A DEFAULT POSITION	20
1. The political economy of data-driven business	20
2. Information as power: data as a pivotal concern in the state-business nexus	22
3. Quantification of the social order	24
4. Complementing the picture: human rights as the reference point for data-driven business	27
4.1. The benefits of a human rights-based approach for data-driven business	28
4.2. The need to better understand the state-business nexus in the data economy	33
III. THE CASE OF DATA DISCLOSURE REQUESTS: A BLACK BOX IN THE STATE-BUSINESS NEXUS	35
1. Situating the socio-political significance of data disclosure requests	35
2. Lack of data to form an empirical basis to evaluate business conduct	36
3. A managerial dilemma: data disclosure requests under a fragmented status quo	37
3.1. A contested legal terrain: data sharing across jurisdictions	37
3.2. Why does a legalistic approach to data disclosure requests not suffice?	38
4. Policy context: governing the gap?	39
4.1. Rights-respecting management based on the UNGPs	40
4.2. Multi-stakeholder efforts on human rights in data-driven business	41
4.3. Persisting loopholes in legal frameworks	43
4.4. Data disclosure requests as a microcosm of digital global governance	44
IV. EXPLORING THE BLACK BOX: MAKING SENSE OF DATA DISCLOSURE REQUESTS	46
1. Sensemaking in organizations	47
2. Data collection	50
2.1. Document analysis	51
2.2. Expert interviews	52
3. Data analysis	58
3.1. Coding of interviews	58
3.2. Retracing the corporate response to data disclosure requests	59

4. Constructing dimensions	59
V. FINDINGS	64
1. Retracing the sensemaking process in companies	64
2. Sensemaking dimensions	68
2.1 External environment	68
2.2. Organizational factors and structures	70
2.3. Shared understanding	74
2.4. Routine for unusual requests	81
2.5. Early actions taken in a moment of crisis	86
2.6. Government relationship	88
2.7. Relationship between headquarters and subsidiary	92
2.8. Human rights mindset	96
VI. DISCUSSION	100
1. Moving from sensemaking to sensegiving: “normalizing the unusual”	100
2. Lifting the corporate veil? Combining local accountability and protection at the group level to respond to complex situations	103
3. How the state-business nexus limits genuine public communications and hinders assessment of whether companies “walk the talk”	106
VII. RECOMMENDATIONS FOR PROGRESSIVE CONDUCT	107
1. Governments - Enable companies to provide transparency in meaningful ways	108
2. Companies - Align the handling of data requests across jurisdictions	109
3. Companies and civil society - Establish an emergency response coordination mechanism	110
VIII. CONCLUSION	113
REFERENCES	118
CURRICULUM VITAE	130

Acknowledgements

I am very grateful for the steady support and outstanding theoretical guidance of Florian Wettstein, whose intellectual rigor, sharp insights and trust continue to be an inspiration of ethical conduct. I would also like to thank my colleagues, in particular Thorsten Busch, Henrietta Dorfmueller, Rose Wangui Kimotho, Kebene Wodajo and Pascal Dey for our stimulating discussions and making the Institute of Business Ethics a great place to work. Further, I would like to thank Isabelle Wildhaber, Antoinette Weibel, Simon Schafheitle, Gabriel Kasper and Thomas Beschorner for their support during our joint multi-disciplinary research project on the use of Big Data in the workplace, and the Swiss National Science Foundation for their generous funding. Cordial thanks to Alexander Tobler for being a witty and reliable PhD companion until the happy end of this journey at the height of a global pandemic.

I am very thankful to Gina Neff for acting as an enthusiastic intellectual beacon and for her invitation to an inspiring research stay at the University of Oxford. My thought-provoking conversations at the Oxford Internet Institute and its community of doctoral researchers remain a fond memory, and I would like to thank in particular Maggie McGrath, Felix Simon and Mona Elswah for their vibrant insights and loyal companionship, and Thomas Vogl for his astute advice. I would also like to thank my wider Oxford network, in particular Jeremias Adams-Prassl for welcoming me into the community of Magdalen College and for his captivating discussion about digital rights, as well as Alexander Henley and Felix Pfluecke for splendid conversations and debates.

I would like to express my great appreciation to all the interviewees who made this research possible in the first place, and made its insights more valuable. Special thanks to my Business & Human Rights “family”: to my former colleagues at the Business & Human Rights Resource Centre, in particular Phil Bloomer for his empowering leadership skills, and to Jonathan Andrew, Samentha Goethals, Dorothee Baumann-Pauly, Catalina Goanta, Frederike Kaltheuner and Gwendolyn Remmert for their valuable reflections. I would also like to thank Annelen Micus, Lisa Hsin and Ekaterina Aristova for inviting me to present my research at the Bonavero Institute of Human Rights. I would also like to thank Adil Hossain and Anneloes Hoff for igniting the spark at the margins of the Oxford Transitional Justice Research group and our workshop on business and human rights during post-conflict transitions, which deepened my interest in pursuing a doctorate.

Last, but far from least, I wish to express my deepest gratitude to my parents, my brother, my partner, and my friends. Thanks to your support, I have found the energy and inspiration to accomplish this work while being separated from many of you due to the pandemic. Thanks to my parents for their outstanding support and having implanted in me strong moral and political beliefs, my brother for sparking my curiosity and interest in technology in our teenage years, and my partner for his love, care and critical reflections along the way. I am so grateful to have you all in my life.

I look forward to the uplifting work ahead!


Isabel Laura Ebert, Zurich, October 2020

Abstract

This research is located in the discourse around structural opacity and the absence of information on the state-business nexus in the data economy. Taking a Business & Human Rights angle and using qualitative research design, this thesis investigates how companies are responding to unusual government requests for user data. Through a sensemaking approach, eight dimensions are constructed that allow one to conceptualize the corporate response to disclosure requests further. The findings show that a persistent frequency of unusual requests can lead to a move from sensemaking to sensegiving, allowing companies to “normalize the unusual”. At the same time, crisis moments persist that trigger sensemaking. Nevertheless, companies increasingly embrace a human rights-based approach through close proximity in management between headquarter and subsidiaries. The findings also depict how the current regulation can constitute a real obstacle to genuine public communication around data disclosure requests.

Summary

User data is an attractive source of information for commercial companies as well as anybody else who might take advantage of its use. Atypical government requests for user data put corporations in a dilemma, in particular in situations where there is limited rule of law, which risks curbing fundamental freedoms, infringing on human rights and challenging democratic governance. Unusual data requests are not only practised by authoritarian regimes but also a practice that liberal democratic states perform, often justified by security narratives. There is very little precise information available on how companies handle such requests; this information would allow for a systemic overview of management practices. This lack of transparency constitutes a black box in the data economy, relating to the wider phenomenon of structural opacity in the state-business nexus.

This research is grounded in the study of Business & Human Rights. It argues that a human rights-based approach in line with the corporate responsibility to respect human rights is best suited to address the adverse impacts of technology companies' activities on society. Using qualitative data from 30 experts working in or with technology companies (telecommunications companies and platforms) and related policy documents, this research explores the corporate response to data disclosure requests from government actors. The qualitative data and related policy documents were collected between autumn 2017 and spring 2020. By exploring the black box of hidden internal procedures and processes in responding to data disclosure requests, this research identifies eight dimensions along which companies are making sense of data requests from government actors: 1) external environment, 2) organizational structures and factors, 3) shared understanding in the organization, 4) routine for unusual requests, 5) early actions taken in a moment of crisis, 6) government relationship, 7) relationship between headquarter and subsidiary and 8) the company's human rights mindset.

The empirical data shows that the emergency situation narrative has become established and has started to move from crisis response to a proactive approach. Further, the findings point to the fact that companies employ a combinatory logic of local accountability and protection at the group level to respond to complex situations. This lifts the corporate veil and demonstrates close proximity between headquarter and subsidiaries around data disclosure requests, whereas distance between these entities is used by companies to relinquish responsibility over their value and supply chain. The findings depict how current regulation can be an obstacle for genuine public communication around data disclosure requests, that does not allow the public to discern whether companies implement rights-respecting practices when dealing with data disclosure requests. Three recommendations are presented: 1. Governments should enable companies to provide transparency in meaningful ways. 2. Companies should align themselves within their respective industry and respective market with regard to their processes on how to handle data requests across jurisdictions. 3. Companies and civil society should establish an emergency response coordination mechanism for dealing with unusual data requests that constitute a salient threat to rights holders on the ground.

Summary in German / Zusammenfassung

Nutzerdaten sind eine attraktive Informationsquelle für viele Akteure. Ungewöhnliche Anfragen von Regierungen nach Nutzerdaten bringen Unternehmen in ein Dilemma, insbesondere in Situationen, in denen die Rechtsstaatlichkeit eingeschränkt ist. Dies birgt Risiken für Menschenrechte und stellt Grundverständnisse der demokratischen Regierungsführung in Frage. Ungewöhnliche Datenanfragen sind nicht nur eine Praxis autoritärer Regime, sondern kommen auch in liberal-demokratischen Staaten vor. Darüber wie Unternehmen mit solchen Anfragen in der Managementpraxis umgehen sind nur wenig aufschlussreiche Informationen verfügbar. Diese Forschung gründet sich auf den Diskurs über strukturelle Intransparenz und fehlende Informationen im Verbindungsfeld von Staat und Wirtschaft in der digitalisierten Wirtschaft, basierend auf der wissenschaftlichen Debatte zu Wirtschaft und Menschenrechten.

Unter Verwendung qualitativer Daten aus Interviews mit 30 Expertinnen und Experten aus Technologieunternehmen, zumeist Telekommunikationsunternehmen und Technologie-Plattformen, sowie relevanten Policy-Dokumenten, untersucht diese Forschungsarbeit die Reaktion von Unternehmen auf Anfragen von Regierungen zur Offenlegung von Nutzerdaten (Erhebungszeitraum Herbst 2017 und Frühjahr 2020). Durch die Analyse dieser "Black Box" der internen Prozesse zu Datenoffenlegungsanfragen werden acht Dimensionen, entlang derer Unternehmen in Bezug auf Datenanfragen von Regierungsakteuren agieren („Sensemaking“) identifiziert: 1) externes Umfeld, 2) Organisationsstrukturen und -faktoren, 3) gemeinsames Verständnis in der Organisation, 4) Routine bei ungewöhnlichen Anfragen, 5) frühzeitige Maßnahmen in Krisenmomenten, 6) Regierungsbeziehungen, 7) Beziehung zwischen Hauptsitz und Tochtergesellschaft und 8) Menschenrechtseinstellung des Unternehmens. Die empirischen Daten zeigen, wie sich der Umgang mit Notsituationen etablierte und den Wechsel von einer Krisenreaktion zu einem proaktiveren Managementansatz. Unternehmen wenden eine kombinatorische Logik der lokalen Verantwortlichkeit und des Schutzes durch die Unternehmensgruppe an, um auf komplexe Situationen zu reagieren. Dies zeigt eine enge Verbindung zwischen dem Hauptsitz und den Tochtergesellschaften im Hinblick auf Datenoffenlegungsanforderungen. Bisher wurde die Distanz zwischen Unternehmensstandorten oder Tochtergesellschaften und dem Hauptsitz von Unternehmen dazu genutzt, die Verantwortung für ihre Wertschöpfungs- und Lieferketten zu verschleiern. Die Ergebnisse zeigen auch, wie derzeitige Regulierungen ein Hindernis für eine transparente, öffentliche Kommunikation im Zusammenhang mit Datenoffenlegungsanträgen darstellen können und es nicht erlauben zu erkennen, ob Unternehmen bei der Bearbeitung von Datenoffenlegungsanträgen Praktiken zur Wahrung von Rechten anwenden. Drei Empfehlungen werden ausgesprochen: 1. Gestalterische Rahmgebung zur Schaffung von Transparenz durch Regierungen für Unternehmen 2. Länderübergreifende Abstimmung zwischen Unternehmen innerhalb ihrer Branche und ihres Marktes zu Prozessen bei Datenanfragen. 3. Koordinierungsmechanismus zwischen Unternehmen und Zivilgesellschaft für Notfallmaßnahmen.

List of abbreviations

B&HR	Business and Human Rights
CJEU	Court of Justice of the European Union
EC	European Commission
ECHR	European Convention on Human Rights
EFF	Electronic Frontier Foundation
ETSI	European Telecommunications Standards Institute
GNI	Global Network Initiative
HRIA	Human Rights Impact Assessment
HRDD	Human Rights Due Diligence
NAP	National Action Plan on Business and Human Rights
OECD	Organization for Economic Cooperation and Development
OHCHR	Office of the High Commissioner for Human Rights
RDR	Ranking Digital Rights
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNGPs	United Nations Guiding Principles on Business and Human Rights

List of figures

Figure 1: The three pillars of the UN Guiding Principles on Business & Human Rights (OHCHR, 2020).....	29
Figure 2: Data sphere between the private sector and states (own illustration)	33
Figure 3: Frame of analysis (own illustration)	47
Figure 4: Abductive approach to sensemaking themes (own illustration)	61
Figure 5 Sensemaking dimensions displayed using the Gioia-Scheme, part 1 (own illustration).....	62
Figure 6 Sensemaking dimensions displayed using the Gioia-Scheme, part 2 (own illustration).....	63
Figure 7: General process model of responding to a request (own illustration)	65
Figure 8 :Process model telecommunications company (own illustration)	66
Figure 9: Platform company process model (own illustration)	67

List of tables

Table 1: Three case studies from the GNI assessment report 2018/2019 (GNI, 2020a).....	16
Table 2: Data sources - triangulation (own illustration)	50
Table 3: Affiliations of interview partners (own illustration).....	54
Table 4: Anonymized overview of interview partners (own illustration)	56

I. Introduction

Technology can be instrumental in realizing human rights 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 (Diamond, 2010, 2015; Lynch, 2011). Particularly in the literature on the Arab Spring, the potential of technology as “liberation technology” has been highlighted (Diamond, 2015, p. 3). This relates to a broader debate about the availability of tech to empower political and social activism and whether it contributes to the emergence of a new public sphere (Lynch, 2011, p. 305; Tsui, 2015, p. 2).

At the same time, sceptics have drawn attention to the fact that tech can also become a “repression technology” (Lynch, 2011, p. 305). For example, new technologies can be used by government authorities for the repression of political opponents: for instance, cases of digital government surveillance of political activists have been documented in countries such as China and Syria (Moss, 2018, p. 267; Qiang, 2019, p. 54). Technology has been a supporting element in enabling human rights abuses, such as through facilitating vast surveillance practices that threaten to silence opposing political voices. As with activists, democratic and authoritarian governments increasingly use the new opportunities that the internet and data offer to achieve their interests (Howard & Hussain, 2011; Lynch, 2011, p. 305).

Digital policy and the global internet have become not just a source of innovation, but also of disruption for society. Transnational flows of data, enhanced by the data collected and processed by modern technologies such as artificial intelligence or machine learning, have the potential to challenge the regulatory and normative cornerstones of global governance (Cukier & Mayer-Schoenberger, 2013; Zuboff, 2019). Adding to this, the separation between the public and private sphere is increasingly blurred, on both an individual and political level – private sector companies and state actors often cooperate closely to govern public speech, monitor election campaigning or adjust economic policy stimuli in the data economy (Ebert, Busch, & Wettstein, 2020; Howard, 2015).

As transnational data flows govern a plethora of processes in the public and private domain, the information connected to such data is a powerful asset. In the midst of this are the government requests for user data that target the private sector. The majority of government requests traditionally were related to interception or the blocking of communication traffic (Tuppen, 2016). In either case, these requests can be targeted towards an individual or a specific website, or extend to mass action across a whole network, such as network shutdowns (Tuppen, 2016). Data disclosure requests by governments focus on the first dimension: data disclosure requests which demand the handover of information (data) obtained and/or collected by companies.

We differentiate between two types of government demand for communications records, as they are used by the telecommunication industry and cyber policy scholars (Bernal, 2016): 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 commonly referred to as “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 commonly referred to as “new surveillance”. In this thesis, I focus on data types defined under b), hereafter referred to either as “user data” or “metadata”, in order to focus on the understudied new surveillance element of data disclosure requests.

The expansion of the internet, and of communications and technology companies and their services across borders in combination with accelerating datafication have disrupted the current governing frameworks that deal with data sharing practices between the private and public sector. There are different kinds of requests and differing degrees of legally-mandated compulsion. The focus of this research lies in government requests for user data that are being labeled by the company as “unusual” and are therefore to a certain extent “unforeseen” or “surprising” in nature. Such requests often occur in a transborder context of conflicting regulatory frameworks and conflicting organizational norms, such as when a local government (host state) requests data that lies in the headquarter (home state) with a particularly tense political setting. In many cases, the regulatory environment of overlapping jurisdictions is politically fraught.

As of today, an effective global framework to govern such data disclosure requests is lacking. A proliferation of regional, fragmented frameworks is rendered obsolete by the fast-evolving datafication of increasingly data-driven business practices and public policy, and also government surveillance. When the government decides to actively tap into data gathered for non-government related purposes, it can reach into the private realm of millions of internet users worldwide. Thus, atypical data disclosure requests disrupt the fundamental understanding of the separation between the public and the private, and pose risks to rights holders – in particular vulnerable groups such as human rights defenders. The international human rights framework, in theory, should provide protection for the right to privacy and all human rights potentially impacted adversely by government data disclosure requests. Nevertheless, under some circumstances, human rights appear to be pushed aside to facilitate a government rationale that justifies intrusion into the private life of an individual or group of individuals. Government data disclosure requests to private companies may entail a loss of transparency for affected stakeholders, and indeed raise questions as to what is actually happening. Such atypical requests, theoretically, occur at moments of crisis or create crisis in organizations. These requests have both legal and ethical implications, with regard to which law is applied and which ethical considerations are taken into account in managerial decision-making.

The ultimate burden is consequently put on the individual company’s practice and the sensemaking (Maitlis & Sonenshein, 2010; Weick, 1988, 1995, 2010; Weick & Sutcliffe, 2001; Weick, Sutcliffe, & Obstfeld, 2005) that precedes it, which lies at the core of this research. The objective of this research is to shed light on the fine balance that internet, communications and technology companies aim to strike when dealing

with data disclosure requests from government: how do companies respond to user data requests from governments? Therefore, this research also explores if and how a human rights lens helps companies make sense and give meaning to these requests and determine how to act in response. To meet the objective of shining light on the space for manoeuvre companies have to react to data disclosure requests, and how their patterns of response differ, the research has to delve into how companies make sense of data disclosure requests by state actors.

Government requests for user data place corporations in a dilemma (Soghoian, 2011, pp. 193-194). Millions of consumers entrust their private communications to companies, and despite public communications about the value of privacy, most firms struggle to discuss the privacy threat posed by government agencies to their customers' data or disclose the degree to which the companies assist or resist such access. At the same time, this does not allow for differentiation among companies with regard to the degree to which companies assist government agencies (Soghoian, 2011, p. 195). The impact of this opaque relationship between companies and governments on data sharing can be particularly severe in situations where there is limited rule of law — which threatens to curb fundamental freedoms, infringe on human rights and challenge democratic governance (Ebert, 2019).

The three case snapshots outlined below provided by the Global Network Initiative (see also II.5.2), a business-led multi-stakeholder platform working on internet freedoms, serve as an illustrative reference point to depict the complex interplay of interests around disclosure requests (GNI, 2020a). The examples below also show that data requests are not only a practice of authoritarian regimes (e.g., that of Myanmar), but also a practice that notionally liberal democratic states (e.g., in western Europe) perform, justified by countering terrorism.

Authority Requests in Myanmar

(GNI, 2020a, p. 22)

This case looked at how Telenor Myanmar (TML) handles authority requests with respect to privacy and freedom of expression.

In 2012, prior to entering the Myanmar market, Telenor Group commissioned BSR to conduct sustainability due diligence, in which privacy and freedom of expression challenges related to authority requests were highlighted. The Telenor Group Manual on Authority Requests applied to TML operations from day one. Although Myanmar's Telecom Law gives the government the right to request confidential information, while protecting basic rights of the citizens of Myanmar, it is not clear on whether the release of confidential information requires a court order. In order to address this issue, Telenor Myanmar built a relationship with the government in Myanmar. The company engaged with authorities responsible for security and police and was able to agree on a set of requirements that would need to be in place in order for the company to respond to a request for confidential information. As an interim arrangement, pending clearer legislation on this area, Telenor established the following requirements: First, all requests to release confidential customer information shall be sent from the police to the telecom regulator for their consent and must include an explanation of Telenor's obligations under the license together with supporting documentation. Second,

independent of the approval from the regulator, Telenor performs its own assessment of each case before deciding to release the requested information or not. A key document as part of this assessment is the First Incident Report which demonstrates that the case has been registered with a Magistrate. In addition, Telenor Myanmar has not turned on the Lawful Interception (LI) capacity in its network until an appropriate legal framework is in place.

Call Data Records Request in Africa

(GNI, 2020a, p. 24)

Orange received demands from the national telecommunication regulator of a country in West Africa. The request was to provide access to Orange's roaming management platform, which contains important customer data on roaming calls.

The regulator asked the company to provide all Call Detail Records (CDRs) in an effort to review and control the tax declaration of all telecommunications network operators. The regulator sent the request in a single letter that it addressed to all four operators in the country. Orange's first response was to pursue a common response from the request recipients to lobby the government or otherwise resist the demand more efficiently. The request recipients sent a joint letter to the regulator in response that noted the lack of legal grounds for the demand, and that the demand was in violation of privacy provisions in national and international human rights law. The government responded by increasing the tax burden for the operators, adding penalties for their refusal to comply with the demand. At this point, Orange alerted civil society organizations about this issue. NGOs denounced the demand on social media and via a letter to the country's Prime Minister. In the end, the government withdrew the demand, while the regulator asked Orange to pay a large fine for not complying. Orange paid the fine to end the case. A positive outcome from the case was that the government made a public commitment to fundamental freedoms. This case is an example of sectoral and multi-stakeholder collaboration to lobby a government to change a policy. The assistance provided by international NGOs and the decision to work with other operators to jointly respond to the government demand clearly contributed to the successful outcome.

Emergency Request for User Data from a Western European Country

(GNI, 2020a, p. 32)

This case examined a company's handling of an emergency

In 2018, the company received an emergency request from a law enforcement agency that has jurisdiction over major crimes in a city in western Europe. The request sought information pertaining to a specific account in order to locate and arrest an individual believed to be planning an imminent terrorist attack in that country. The request was in writing on the law enforcement agency's official letterhead and signed by an appropriate official. It was transmitted in its original local language accompanied by an English translation. The request sought basic subscriber information for a particular account as well as additional contact information and IP logs. The request was reviewed pursuant to the company's procedures. Finding that the request pertained to a bona fide

government request for information of an email user in a western European country. This was part of an effort to locate and arrest an individual suspected of planning an imminent terrorist attack.	emergency involving the potential of significant loss of life, the company responded by disclosing the basic subscriber information it possessed regarding the specified account to the law enforcement agency. This case illustrates a company's policies and procedures for responding to emergency requests from governments. It shows the functioning of a company policy of responding to such requests with the least amount of data required to respond to the emergency. There is always a concern that governments may misuse these emergency requests to obtain data from companies in situations that do not meet the stringent criteria for such emergencies. Providing the minimal amount of responsive data that is reasonably connected to the government's objective provides an appropriate safeguard against the possibility of misuse.
--	---

Table 1: Three case studies from the GNI assessment report 2018/2019 (GNI, 2020a)

As these cases show, regardless of governance frameworks, atypical government requests for data disclosure create equivocal situations that have legal and ethical implications and engage companies' (human rights) responsibilities (Parsons, 2019). Whether they occur in periods of crisis or during business-as-usual, in democratic or authoritarian contexts, such ambiguous and complex situations require sensemaking of data disclosure requests. As such cases are scarcely documented in the media or in scholarship (Soghoian, 2011), there is little knowledge of what occurs within the black box of corporate sensemaking when deciding to decline or respond to an atypical request. As of yet, this question has not been addressed from a scholarly perspective, let alone from an angle focussed on human rights and business. The goal of this thesis is to open up the black box of corporate decision-making on data disclosure requests and to comprehend how businesses approach such sensitive situations, particularly while keeping in mind their implications on human rights. Gaining a better understanding of the processes through which technology companies make sense of these requests and use human rights principles to help them take and enact responsible decisions is at the core of this research. This thesis makes a novel and innovative contribution by allowing for a better understanding of internet governance in the state-business nexus, at the very core of which stand data-sharing practices between the private and the public sector. Government requests for user data are the vanishing point for analysing power relationships between multinational technology companies and states. Surveillance of metadata can render people more vulnerable and expose them to a heightened risk of human rights abuses, for example online intimidation and threats against human rights defenders and/or ethnic, racial or religious minorities, and related unfair trials or imprisonment. In conflict zones, which by their very nature expose individuals to higher human rights risks, governance of such data needs to take into account what harm can result when technology companies share data with conflicting parties. The vast amounts of data that the dominant businesses in the technology sector hold attract many states' attention. While some requests might be connected to appropriately-justified law enforcement purposes, other requests will simply endanger rights holders, including

those fleeing from political persecution, by laying bare the very information that government actors need to silence dissenting voices.

This research study explores the space for action that companies have to respond to such requests and what actually happens inside a company when a request comes in from the government for user data. Using qualitative data collected from 30 experts working in or with technology companies (for the most part classified as telecommunications companies and platforms), and related policy documents collected between autumn 2017 and spring 2020, I argue that the corporate response to data disclosure requests from government actors can place companies in a dilemma, in particular when dealing with atypical data requests from government actors. Where companies need to hand over data, legal requirements or license agreements (in particular telecommunications companies) often mean their room for manoeuvre is limited. Yet companies also enjoy considerable leeway in how to react to unusual data requests, and which strategies they choose to employ in response. The research permits the gathering of further insights into the differences and similarities of how companies respond to government requests for user data, thereby allowing a more differentiated view of actual company practice and the extent to which companies aim to resist requests, and under what circumstances.

The research connects to an existing debate around the role of data in the opaque structures of the state-business nexus and its adverse impacts on society (Eubanks, 2018), a society constituted of a range of “black boxes” (Pasquale, 2015). Through exploring the “black box” of data disclosure requests, this appraisal empirically assesses how businesses aim at implementing rights-respecting practices (Obara, 2017) in the data economy when cooperating with state actors. It further contributes to research in organizational studies as to how companies aim at making sense of adverse events in crisis and how they react to them (Maitlis & Christianson, 2014; Maitlis & Sonenshein, 2010; Weick, 1988, 2010; Weick & Sutcliffe, 2001) by depicting how a macro-social structure of government agencies and conflicting legal frameworks influences sensemaking in organizations. Adding to this, the research responds to a strong call for studying the management of human rights in business implementation (Schrempf-Stirling & Van Buren, 2017; Wettstein, Giuliani, Santangelo, & Stahl, 2019). It contributes to the emerging literature on the processes through which individuals from local country management to the senior management level become aware of human rights issues (adverse impacts from data disclosures) that affect their organization (Goethals, 2019; Obara, 2017; Obara & Peattie, 2018). The research forms a basis from which to further theorize how business aims at mainstreaming human rights considerations into decision-making processes in high public pressure situations (Schrempf-Stirling & Van Buren, 2017).

The thesis also responds to two limitations that have characterized the academic Business & Human Rights (B&HR) discussion in the past, the first relating to the subject area of new technologies and the second to empirical methodology (Deva, Ramasastry, Santoro, & Wettstein, 2019). Firstly, the thesis addresses the implications on human rights of the conduct of ICT companies, through studying the specific issue of data disclosure requests and their human rights impacts as well as the managerial

response. Secondly, while B&HR has focussed on conceptual scholarship, argumentation, and rather doctrinal analysis of new policy developments or normative assessments of company conduct in a range of contexts, this thesis empirically investigates the mechanisms that translate new policy developments into improving the situation on the ground and how companies aim to contribute to responding and solving these issues (Deva et al., 2019). Through an empirical approach, the research sheds light on the ways in which individuals raise awareness of human rights in companies, and take action and respond to emerging human rights issues (Schrempf-Stirling & Van Buren, 2017). The research connects to the existing small body of literature using human rights as a sensemaking framework in the field of business and human rights (Goethals, 2019; Obara, 2017; Obara & Peattie, 2018) and allows the empirical basis of corporate management strategy to extend to human rights. The findings thus offer grounds for further theorizing how the business and human rights framework is transposed into business situations in the digital economy and whether it challenges previous assumptions of business behaviour in the state-business nexus. Furthermore, this research can also add value to critical data studies by enhancing the empirical basis for reflection on the normative implications resulting from current management practices by telecommunications companies and platforms (Jørgensen, 2018, 2019; Kotliar, 2020).

In the following chapter (II.) I will sketch the default position on the necessity of opening black boxes in the data economy (Pasquale, 2015), touching upon the political economy of data-driven business and why “information is power”. Furthermore, I discuss how data can prove pivotal in the development of the nexus between state and business, and how the quantification of the social order contributes to this phenomenon. I close with a strong call for recognition of human rights as the reference point for data-driven business and the need to better understand the state-business nexus in the data economy. The third chapter (III.) depicts the case of data disclosure requests as pivotal in the state-business nexus by situating the socio-political significance of data disclosure requests and sketching the current mixed empirical evidence on business conduct in that area, illustrated by the sparse account of actual company behaviour that is retraceable in the current state of research (Parsons, 2019; Rahman, 2016; Soghoian, 2011). Further, the fragmented framework of data disclosure requests is discussed from a legal angle (A. K. Woods, 2017), concluding that a legalistic approach does not suffice to protect human rights when dealing with unusual data disclosure requests from governments to companies. The chapter closes with a brief depiction of the policy context that aims to close the governance gap, sketches the progress made on rights-respecting management in digital global governance, and reviews how policy-makers push forward while claiming that certain loopholes still persist when processing unusual transnational data disclosure requests. This then leads to the fourth chapter (IV.), the empirical part of the paper that explores the black box through a qualitative research design based on sensemaking and crisis. It lays out the methodological considerations, data collection methods (by data triangulation of policy documents and expert interviews), and elucidates the sampling strategy. The data analysis explains how data patterns are identified as sensemaking patterns, using sensemaking as a theoretical framework that is used to address crises and ethical dilemmas. The fifth chapter (V.)

presents the findings in line with the eight constructed sensemaking dimensions. The discussion (VI.) anchors the research within the sensemaking and sensegiving literature by showing how companies slowly move from sensemaking to sensegiving when responding to data disclosure requests from governments. It also connects to the business and human rights discourse by showing how the close interaction between headquarter and subsidiary opposes the perception of the headquarter having weak leverage with its subsidiaries. It further discusses how current frameworks hinder companies from sufficient public discussion of their stance towards responding to data disclosure requests and how this leads to tensions between internal and external communications. The recommendations are presented in chapter VII. They call for better enabling of corporate communications on disclosure requests, lay out concrete recommendations for best practices to respond to disclosure requests in rights-respecting ways, and highlight the need for the establishment of an emergency response coordination mechanism to protect rights holders from salient harm. The last chapter (VIII.) provides final reflections and conclusions.

II. Opening black boxes in the data economy as a default position

1. The political economy of data-driven business

Business tends to embrace innovation, and corporate innovation has led to historic re-adjustments of the market. Some less drastic changes and some more fundamental ones have been caused by scientific and technological progress over the decades. The past decade has certainly been characterized by a boom in the digital sphere (Cukier & Mayer-Schoenberger, 2013; Mayer-Schönberger & Ramge, 2018). The so-called data economy is an economy that relies heavily on the collection, processing and analysis of vast amounts of data. This chapter will explore “what’s new” for human rights in the data economy, especially with regard to the state-business nexus. Here, I ask, do we need to raise anew fundamental questions about the role of the state in relation to the private sector and companies? Moreover, how does data as a “commodity” come into play here?

No matter the intended 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 (Neff & Nafus, 2016). This data and societal “datafication” process allows in-depth insights into users’ private and professional lives, political opinions, social and professional circles, patterns of consumption, and geographic location (Cukier & Mayer-Schoenberger, 2013). The accelerating effects of datafication and data maximization, driven forward by new mechanisms for data gathering and interpretation as well as the rise of artificial intelligence, push deep into society and business (von Krogh, 2018). Data profiling of individuals has become easier, cheaper, and widespread: as a consequence, a new information phenomenon emerges (Gasser & Almeida, 2017). The granularity and scalability of gathered data can serve various interests in both the private and public sector. In this regard, Zuboff (Zuboff, 2015, 2019) argues that data sharing between the private sector and the public sector is creating increasingly blurry interlinkages and enabling a form of government-surveillance complex. Relatedly, the growing “commodification” of the individual through data sharing has been shown to put vulnerable groups in a weak position and threatens to disempower marginalized voices, especially in the context of autocratic regimes (Deibert, 2008, 2015a, 2019; Elswah, Howard, & Narayanan, 2019; O’Neil, 2017). The increasing appetite for data-based insights in both the private and the public sectors holds important implications for companies’ responsibilities which require an adaptation of practice (Ebert et al., 2020).

Information and communication technologies have been discussed as an ambivalent phenomenon in political science and legal studies. The narrative of technology as a tool of liberation needs to be contrasted against the frequency with which the very same technology is used to facilitate repression (Diamond, 2015; Lynch, 2011). The narrative around technology as a tool of liberation evolved strongly in connection with the so-called “Arab Spring”, when protesters mobilized through social media, demanding changes to their political regimes and being partly successful in those demands. At the same time, research has shown that the data gathered from social

media and other data sources can be used against citizens, either through government surveillance tactics, misinformation campaigns or hate speech (Alimardani & Milan, 2018; Elswah et al., 2019).

In general, the accelerating speed of technological progress enables the collection, processing and analysis of more and more granular and complex data (Gasser & Almeida, 2017). At the same time, increasing datafication can have a plethora of intrusive effects as the data can convey profound insights into people's lives. The impact of new technologies on privacy, freedom of expression, labour rights, and discrimination against populations and individuals based on race or gender has been in the spotlight in critical data studies (boyd & Crawford, 2012; Cohen, 2012, 2016; Graham, Hjorth, & Lehdonvirta, 2017; Noble, 2018; Zuboff, 2015, 2019). On a legal and political level, the increasing amounts of data, the availability of cheap analytics technologies, and their use in daily business in combination with cross-border data exchanges, leads to an even more complex appraisal of jurisdiction and interferences related to established norms in a global context – thereby potentially undermining the existing legal framework (boyd & Crawford, 2012; Crawford & Schultz, 2014; Ebert et al., 2020; Mittelstadt, Allo, Taddeo, Wachter, & Floridi, 2016; Prassl, 2018; Richardson, Schultz, & Crawford, 2019; Wachter, 2018; M. Whittaker et al., 2018). Nevertheless, the “digital space” is not an alternate sphere that exists beyond laws, norms or principles but should in theory always be bound by the same conditions as the enjoyment of rights in “physical places” (Graham, 2019).

The disrupting effects of the use of technology can challenge human rights protection, as recent scandals around censorship, network shutdowns, data breaches and data exchanges of user data without “user consent” have shown (Deibert, 2008, 2015a, 2015b, 2019; MacKinnon, Hickok, Bar, & Lim, 2015; Maréchal, 2015; M. Whittaker et al., 2018). Among various other smaller scale scandals, a major incident in recent years was that involving Cambridge Analytica in 2018. The Cambridge Analytica scandal revealed that the Cambridge psychologist Aleksandr Kogan used personal data that Facebook had been harvesting from millions of its users through their user profiles (Confessore, 2018; Glasius & Michaelsen, 2018, p. 3789) for profiling without user consent. This data had then been used for political purposes, such as influencing voter behaviour through targeted advertising.

The Cambridge Analytica case can also serve as a point of reference to illustrate how state actors, private sector companies and academia cooperate closely to spearhead technological innovation in the field of data mining, data science and similar fields of application (Howard, 2015; Mayer-Schönberger & Ramge, 2018; Mazzucato, 2011; Moore & Tambini, 2018). The work of Howard (2015), Mazzucato (2011), and Moore and Tambini (2018) point out that corporate power in that area resembles an oligopoly of “Digital Dominance”, with a small set of companies setting the agenda and determining the path of technological innovation. Framing this notion in an even more critical light, certain scholars have argued that we have entered an age of “surveillance capitalism” (Zuboff, 2015, 2019) or “platform capitalism” (Srnicsek, 2017). Similarly, Cohen introduced the notion of a “surveillance-innovation complex” (Cohen, 2016), relating to issues such as public-private partnerships not only within the justice

system, but also with respect to the increasingly wide-spread use of surveillance technologies in public contexts, or in the influencing of election campaigning (Eubanks, 2018; O'Neil, 2017). In their ongoing efforts to become ever more competitive and innovative, international corporations appear to leave no stone unturned to uncover the hidden potentials of the data economy.

Despite differences in the extent of criticism targeted toward certain actors, there has been a movement to acknowledge that a small set of technology companies hold the key assets, power, and knowledge to shape the “datafication” of the economy. This has consequences far beyond the economic sphere itself. It can fundamentally change our social order, as I will argue in the discussion that ensues in this review. Datafication has started to re-define and re-structure our understanding of public governance frameworks and the functions of government too. The balance between the government’s legitimacy to enforce human rights in the online sphere has shifted remarkably towards dependency on a company’s will to implement protective measures – content moderation being just one of many examples (Gillespie, 2010, 2014, 2018). In addition, for instance, Amazon, Facebook, Google and Microsoft continue to be heavily criticized, both by the media and their own employees, for cooperating on morally questionable government projects including facial recognition, border policing, drone surveillance, and the policing of refugees and/or marginalized communities (Ebert et al., 2020). Corporate practices facilitated by technological progress can have adverse impacts on human rights. In particular, from an intersectionalist and feminist perspective on gender, race and inequality, authors have documented these adverse impacts on the enjoyment of human rights and are calling for a novel framework to govern structural injustices in the technology sector and its impacts beyond the industry (Benjamin, 2019; J. Buolamwini, 2018; Joy Buolamwini, 2018; Buolamwini & Gebru, 2018; S. Costanza-Chock et al., 2018; Perez, 2019).

2. Information as power: data as a pivotal concern in the state-business nexus

Taking a step back, technology has been facilitating communications since the telegram was invented, moving on to telephones, smartphones, and other computing-facilitated forms of communication. Similarly, the monitoring of communications has been a practice that goes back more than a century: governments have long understood how information furnishes power – think of the use of surveillance during the German Democratic Republic (GDR) and the Staatspolizei (or “Stasi”, German for state police) (Koehler, 1999). However, surveillance practices reached a new level in the wake of anti-terrorism efforts, in particular post 9/11, and increased digital communication. Technological innovation has made interception and monitoring practices cheaper but also more insightful as the quality of information collected from communications has increased (Greenwald, MacAskill, & Poitras, 2013). The leaks by former intelligence employee Edward Snowden have demonstrated the extensive level of data sharing between the private and public sector, as triggered by a national security narrative. These practices have come to increased public attention since the

revelations by Snowden and others, which heavily criticized the mass surveillance carried out by US intelligence agencies (Greenwald, 2015; Greenwald et al., 2013).

However, data requests from governments to gain access to data in the private sector have been used as a political tool well before the heightened state of national security after the terrorist attacks of 9/11. One of the key cases to emerge involved the US internet company Yahoo!'s Beijing subsidiary handing data over to China, which led to the arrest and alleged torture of the Chinese journalist Shi Tao in 2005 (MacKinnon, 2012). For many companies, in particular US-based ones, this was a wake-up call for corporate awareness with regard to complicity in human rights abuses through the contribution to data disclosure practices. A subsidiary of Yahoo! in Beijing had complied with a Chinese data disclosure request, deemed as valid, for user account data that offered the evidence required for the police to arrest Shi Tao and sentence him to 10 years in prison (MacKinnon, 2007, 2011; Samway, 2016). Shi Tao is said to have faced intimidation and torture by authorities as he was accused of disclosing state secrets by sharing his notes about official Chinese press coverage rules set by the Chinese government on reporting the 15th anniversary of the Tiananmen Square protests with a US website (Israel, 2009). This case made many companies realize that, besides the vast global expansion of US tech companies in the early 2000s, global governance questions might become more troublesome due to the nature of a US-centric understanding of laws governing the internet space conflicting with other countries' domestic laws and practices, as well as the evident friction in respect of international law (Israel, 2009; Samway & Ryan, 2014). As the examples in the introduction from Myanmar, western Europe and west Africa have illustrated, such intricate situations are in no way a novel development, yet continue to pose difficult questions to company executives and staff on the ground. They also continue to threaten the rights of vulnerable individuals and groups – although it may be acknowledged organizational learning might have led to some companies to finding novel answers to persistent questions.

It is noteworthy that today's technological capacity is different to that of the past, during the time of the GDR, for instance. Today, metadata can be just as revealing as content data due to the use of smartphones and similar technologies providing insightful data, including geolocation, biometrics (including facial recognition and/or fingerprints), and permitting advanced levels of aggregation and analysis (Bernal, 2016, p. 246f; Neff & Nafus, 2016). Hence the "new" surveillance by metadata differs in quality and quantity from "traditional" surveillance or interception of communications (Bernal, 2016, p. 247f). With regard to Article 8 of the European Convention of Human Rights (ECHR) for example, new forms of online communications increase the spectrum of relevance and scope, also affecting human rights other than privacy (Bernal, 2016). In the age of datafication, metadata is a valuable resource for surveillance purposes as it can be more easily analyzed and aggregated than content; formats are standardized, often numeric, and hence are a viable basis for quantitative analysis (Bernal, 2016, p. 248). Often, the data held by corporations is of much better value for the government than the data the government would collect itself, due to its granularity and scale as a result of data maximization business practices. Hence there is a large appetite on the part of government to tap

into corporate data assets. In this context, the national security narrative is a double-edged sword for many human rights defenders. Grabenwarter (2014) outlines the balancing act required to avoid infringing on user privacy whilst guaranteeing national security. At the same time, a national security narrative might be used to disguise the government's actual intention in terms of the proposed use of the data (Ebert, 2019).

3. Quantification of the social order

It has become evident that data-driven business affects lives on many levels and in a wide range of contexts. The data economy is built on a constantly increasing pool of data and a vast data infrastructure, with quite a centralized technological avant-garde which holds key decision-making power and storage capacities. This has produced some questionable, opaque new inter-dependencies between the state and the private sector. This complex system is characterized by structural opacity made up of a plethora of "black boxes", which led Pasquale to coin the term "black box society" (Pasquale, 2015). Pasquale defines a "black box" as a metaphor that with its dual meaning relates to either a recording device, like a data monitoring system, or a "system whose workings are mysterious; we can observe its inputs and outputs, but we cannot tell how one becomes the other." This allows one "to scrutinize the others while avoiding scrutiny oneself," which is "one of the most important forms of power" (Pasquale, 2015, p. 3). Black boxes are characterized by real secrecy, establishing barriers of access the black box (such as a "key" for a "door"), legal secrecy, referring to laws that keep information secret, and obfuscation, which is the deliberate attempt at concealment if real or legal secrecy have been compromised (Pasquale, 2015, p. 6).

The data economy builds on the underlying belief that the social lifeworld in a Habermasian sense can be represented in a quantified version displayed by data traces (Cukier & Mayer-Schoenberger, 2013; Habermas, 1981; Mau, 2019; Porter, 1986, 1996; Van Es & Schäfer, 2017). At the same time, data-driven societal models and quantified conceptualizations of human life are not immune to errors or false conclusions about human interaction, and these faulty conclusions in combination with opaque modes of interaction between key actors can result in a range of societal issues (Neff, Jordan, McVeigh-Schultz, & Gillespie, 2012; Pasquale, 2015). Two examples illustrate potential faulty conclusions derived from quantified conceptualizations. A client of a bank can receive a negative credit rating because they live in an area where the postcode is historically associated with low-income households and crime, despite the fact that the client has sound finances (O'Neil, 2017). Or, women and people of colour are screened out of a hiring process of an IT department due to their skin colour or gender, despite being professionally well-qualified for the job role. Most likely, the hiring algorithm was trained on historic data that postulates that white, male candidates over the age of 40 constitute the population group that should be hired, as these characteristics in the past were most evident amongst the previous employees in the IT department (DeBrusk, 2018; Ebert et al., 2020). These are examples of how faulty (and discriminatory) practices based on gender and/or race or social economic background may manifest in data analytics.

Fundamentally, relying on such quantified, calculative practices has the potential to transform how we understand our social order, what we attend to, and how we organize our lives (Mennicken & Espeland, 2019, p. 224). Why is this the case?

“Data universalism” as conceived by Milan and Treré (2019), neglects the contextuality of human life, such as cultural boundaries or social notions, and the data traces it produces. Certain “externalities” are not considered in data models. Data universalism describes an assumed default position based on Western-centric assumptions as to how society can be quantified and transposed into data models and data-driven business models, and therefore highlights the need to develop a concept that can also embrace the local contexts in the global South (Milan & Treré, 2019; Ricaurte, 2019; Taylor & Broeders, 2015), and refrain from normatively “Othering” or “westernizing the Other” (Kotliar, 2020). Quantification affects power and politics by shaping relations of visibility, determining what gets noticed and what does not, and potentially neglecting the complexity of causal connections of social phenomena (Mennicken & Espeland, 2019, pp. 225, 228). Human rights play an increasingly vital role in setting boundaries as to the extent human life can and should be captured in data, how this data is collected and analyzed, and which decisions are taken based on such an analysis. Mennicken and Espeland (2019, p. 232) point out three important implications for critically looking at the quantification of the social: (1) incorporation of the voice in numbers: an examination of the conditions and possibilities of public participation, and the inclusion of local knowledge in indicator design; (2) pluralization of quantification: the development of alternative measures (counter-quantifications) to irritate, unsettle, and destabilize existing quantifications; (3) the relationship between quantification and public debate: what role do statistics play in generating and framing public discussion and deliberations around public goods?

A critical reflection about the necessity of quantifying every “fiber” of human life and the limits of the representativeness of such derived numbers serves as an important deterrent for the data economy from entering full-swing “surveillance capitalism” (Zuboff, 2019). 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 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 (Ebert et al., 2020).

This socio-technical embeddedness of data in the social order of individual and collective lifeworlds becomes clearer when looking at the two data subject groups of social media users and employees in the section below, and the sort of information this data can reveal. Both users of platforms and, increasingly, employees are interesting providers of data for analytics and predictions. Many users engage in extensive self-tracking activities that collect vast amounts of data, in particular personal metrics, such as through health apps on smartphones (Neff & Nafus, 2016). Web browsing data can be used to get insights about intimate, personal information, more than might be obvious at first sight: visiting certain websites, searching for

specific terms, clicking on particular links, downloading various documents, as well as the length and frequency of website visits combined with the kind of device used for these purposes (Bernal, 2016, p. 253). 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 (Bernal, 2016, p. 253).

Many social media platforms do not charge for the use of their services but instead require users to accept vast behaviour tracking practices across their platforms. Data collected by social media platforms such as Facebook or Twitter with its group communication tools might create privacy issues that make activists easy targets for police forces in oppressive regimes (Bernal, 2016). As described earlier, social media platforms used to be praised as “liberation technologies” during the revolutions in countries such as Egypt in 2011, raising hopes of the positive effects on freedom of speech and democratization through online discourse (Diamond, 2010, 2015). However, in recent years, these same platforms have become a severe threat to activists and human rights defenders because their policies and design decisions endanger rights holders when the data collected on the site can be used as “digital evidence” against them (Lynch, 2011). For example, in the case of dating apps, such data was used against members of the LGBTQ community. The data logs made users vulnerable to government abuse as the use of the app revealed their sexual orientation in an environment where the political and criminal law context is such that members of the LGBTQ community expressing their sexual identity may in practice be subject to persecution (Rigot, 2018).

Also, companies are increasingly monitoring the behaviour and performance of their employees at the workplace (Prassl, 2018). It is not only modern gig economy platforms that monitor their employees on a minute-by-minute basis. Rather, monitoring at the workplace, sometimes equaling corporate surveillance, has a long history at call centres and in other service industries, such as UPS delivery services or Amazon warehouses (Ball, 2010). The accelerated data economy puts new pressures on traditional companies to monitor their employees in the workplace, extending the object of monitoring/surveillance from blue-collar workers to include white-collar office employees. Research has shown that the use of monitoring technology can change patterns of social interaction at the workplace (Kellogg, Valentine, & Christin, 2020).

The experience with both data subject groups shows how the depth of data information available about an individual will be increasingly vast, and the relevance of protecting such data is steadily growing in importance. Lifting this to a more philosophical level, the notion of a “technocratic consciousness” is becoming the leading productive force in societal life and threatens to diminish the free, open and communicative character of the “social lifeworld” through the realm of technological control (Habermas, 1970, 1981). Habermas (1995) builds on a deliberative model of democracy and the pivotal concern here is that constructing the social order through technology and its unbalanced power structures might inhibit an inclusive deliberative discourse from representing a balanced range of voices. This “technocratic

consciousness” also relates closely to an inherent tension in the state-business nexus between the appetite of government actors to use data partly gathered by their own institutions and/or obtained from the private sector for beneficially shaping better policy and implementation strategies, and their state duty to protect their citizens’ freedoms online. As key actors in the data economy struggle to address their adverse impacts on society, a human rights framework can constitute an important protective mechanism (Habermas, 1995, p. 102f.) to re-evaluate and adjust business models and operational practices. In the following discussion we shall explore why human rights are critical in striking a new balance of interests in a data-driven business environment.

4. Complementing the picture: human rights as the reference point for data-driven business

For many decades, human rights have remained a complicated undertaking in global governance due to conflicting normative beliefs. The political agenda after the Second World War introduced far-reaching promises of global prosperity through global trade and economic growth. Nevertheless, leading economists and political scientists have not ceased criticizing the global economy for systemically turning a blind eye to key governance gaps, such as questions of justice, including questions of basic human dignity (Dingwerth & Pattberg, 2006; Keohane & Nye, 1977). Global justice in trade relationships and a connected development policy narrative shows a fragmented picture. Historic examples include the deprivation of countries in the global South of their natural resources by colonial powers and the financing of conflicts through business with armed groups (Collier, 2008; Collier et al., 2003; Frank, 1966; Sachs, 2006). The economic incentives of conducting global business increasingly lead to a disconnect between societal needs and the outcomes of the economy (Peet & Hartwick, 2015; Wettstein, 2009). Drawing the economic inequalities down to the individual level, this has ultimately created a governance gap in the protection of human rights. Scholars first started to discuss business responsibilities for human rights systematically in the mid-1990s (Chandler, 2003). Due in part to tensions in different interpretations of human rights, for example in respect of the power of companies and the effects on state sovereignty, scholars such as Alston and Clapham have argued that companies as non-state actors hold far-reaching powers that impact human rights, and have thus asserted that they have an obligation to respect human rights (Alston, 2006; Clapham, 2006). In particular, the operations of multinational enterprises often extend beyond the regulatory reach of individual governments and can create governance gaps between economic and political globalization processes (Macklin & Simons, 2014). Economists (Sen, 1999) started to discuss how an economic system needs to be designed that serves the people first, and tailors business incentives to serve this purpose (Ulrich, 2008). Such calls for a re-adjustment of the economic system were followed by a discourse arguing that corporations have become de-facto political actors, and, as a result, businesses have political responsibilities within the economic system (Scherer & Palazzo, 2011).

Today, not only certain commodity-based business transactions and governance relationships, but also data-based economic networks, have been characterized by

an increasingly unbalanced distribution of power across the globe. That is why scholars have coined terms such as “data colonialism” (Couldry & Mejias, 2019) to describe how a technologically-driven economic logic increasingly views human life as a basis of data extraction. Certain scholars (Ricaurte, 2019; Sadowski, 2019; Taylor & Broeders, 2015) argue that “Western” powers, as the main agenda setter, neglect contextuality such as culture, politics, local customs and unintended consequences when implementing a universal business model worldwide. In the next section, I discuss how a human rights-based approach could create more inclusive operating models in the data economy that benefit the notion of the human rights responsibilities of business when transposed into the realities of the data economy.

4.1. The benefits of a human rights-based approach for data-driven business

It has become apparent that through the datafication of as many aspects of business and society as possible, companies affect human rights on various levels and in a wide range of contexts. Digital business practices impact society, and on a more localized level, human rights too – as with the economic power dynamics historically associated with commodity-based trade and business relationships (Ebert et al., 2020). However, consensus on how to address the potentially negative impacts on society of these business practices in the digital sphere is not yet clear-cut. Concepts which are solely based on ethics or ethical guidelines have been criticized for their voluntary nature and vague language (Raso, Hilligos, Krishnamurthy, Bavitz, & Kim, 2018; Sloane, 2018). Among others, Wagner (2018) argues that the vague language of corporate social responsibility (CSR) is frequently used by corporations to avoid regulation in the digital space.

Rather, I argue, the literature demonstrates that addressing corporate responsibility in the digital sphere through a business and human rights perspective has strong benefits. The academic Business and Human Rights (B&HR) debate relates closely to the result of a decade-long process at the level of the United Nations (UN) to better define the responsibilities of business towards human rights, which reflects the academic debate around governance gaps in human rights protection. It has also started to tackle technology-related human rights issues.¹

The basis of the B&HR framework are the non-binding United Nations Guiding Principles on Business and Human Rights (UNGPs), a soft-law instrument (UN Human Rights UN, 2011). 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.

¹ For the policy context related to the academic debate on B&HR, please see chapter III. 4.

THE GUIDING PRINCIPLES THREE PILLARS



Figure 1: The three pillars of the UN Guiding Principles on Business & Human Rights (OHCHR, 2020)

The B&HR lens offers three key overarching benefits to address the state-business nexus in the data economy: 1) B&HR is anchored in universally-accepted norms which allows for shared understanding among actors and strong accountability mechanisms 2) as a practice-oriented approach, B&HR offer precise tools and instruments for implementation in business operations; and 3) B&HR conceptualizes the relationship between the state and private actors around human rights, providing a sufficiently non-static perception of the relationship which allows space to deal with emerging tech-related human rights issues. In the following, I elaborate on these three overarching benefits.

1) B&HR situates the debate around the responsibility of technology companies in internationally established norms and universally accepted human rights (Baumann-Pauly & Nolan, 2016; Ebert et al., 2020). While the Universal Declaration of Human Rights (UDHR) laid important groundwork on the state role to protect human rights, policy makers recognized the increasing impact that corporate activities can have on the enjoyment of those rights. B&HR has strong anchors in the UDHR and the duty to protect human rights is clearly understood to rest with the government as incorporated in international law (De Schutter, Ramasastry, Taylor, & Thompson, 2012; Deva, 2003; UN Human RightsUN, 2011). This anchoring of B&HR in international law makes it potentially stronger for accountability mechanisms than, for example, ethics-based approaches (Ramasastry, 2015). Such stronger accountability is what many interdisciplinary researchers in technology studies have been calling for (Benjamin, 2019; Buolamwini & Gebru, 2018; Sasha Costanza-Chock, 2018). To a certain degree, B&HR stretches the normative understanding of the state as the duty bearer to protect human rights under international law by extension of a soft-law component of corporate responsibility for businesses. Yet, B&HR does not add new a legal dimension, but rather works via a postulated shift of the normative concept of the corporation in society. Companies have the responsibility to respect human rights throughout their operations based on a continuous risk management process to

identify, prevent, mitigate, and to be held accountable for addressing its human rights impacts (Addo, 2014). Adding to this, access to a remedy should be provided by judicial means by the state in relation to the state duty to protect, or by non-judicial means, such as company-level grievance mechanisms (Deva & Bilchitz, 2013).

2) Originally grounded in legal scholarship, but increasingly also expanding into organizational studies and related fields, the B&HR approach provides a focused and practice-oriented angle. As a result, B&HR offers tools and instruments, such as human rights impact assessments (HRIA), as concrete ways to align human rights with the core of the business processes in companies (Wettstein, 2016). Human rights here serve as a “targeted reference point for practical tools and initiatives” (Wettstein, 2018, p. 82). While more sector-specific best practices are emerging, a continuous exchange among stakeholders lays the foundation for so-called “Human Rights Due Diligence” (HRDD) as an ongoing risk assessment process aimed at creating awareness of human rights issues, and preventing and addressing adverse impacts, including communicating about them and integrating feedback loops (Baumann-Pauly & Nolan, 2016; McCorquodale, Lise, Neely, & Brooks, 2017). This also means that companies finding themselves in different positions within the value chain need to be part of this process. It is not only applicable to transnational corporations but also to small and medium-sized enterprises, including their co-dependencies with larger players in the field. While B&HR frameworks offer a “do no harm” perspective as a minimum standard to avoid negative effects on human rights through business operations (Ruggie, 2007, 2013; Wettstein, 2015, 2016), B&HR also recognizes that it might not always be possible to fully anticipate harmful effects. Identifying and managing human rights risks can become a challenging task in the tightly-knit web of the data business-state nexus (Howard, 2015; Mazzucato, 2011; Moore & Tambini, 2018). B&HR is useable and designed along existing risk management processes (Fasterling, 2017). It offers both a management practice that follows a process-based approach with a proactive, steadily ongoing and preventive approach towards human rights protection, and stresses the importance of mitigating and remedying harm caused by business activities (Baumann-Pauly & Nolan, 2016; Santoro, 2015).

3) It is of additional benefit that B&HR, to a certain extent, does not rely too heavily on a functioning state order. Recognizing rule of law issues in a number of jurisdictions, it postulates that even when the state fails to uphold its state duty to protect, a company has to carry out its responsibility to protect human rights (Martin-Ortega, 2008). B&HR, in that regard, can embrace a non-static view of a company’s role within a societal system that does make it necessary to engage with the role of the state to protect human rights (Wettstein, 2015). For example, if a business operates in a jurisdiction with weak governance, B&HR offers guidance on how the company should act with regard to its human rights responsibilities (Martin-Ortega, 2008; Michalowski, 2014). This dynamic perception of a company’s role appears as a suitable fit to the fast pace of the digital space and the, at times, fast-evolving data ecosystems, which can make it necessary to constantly redefine boundaries between the state duty to protect human rights and the corporate responsibility to respect human rights.

Precisely, what B&HR offers is an orientation of how to operationalize human rights in a business context, also applicable to business activities' impacts in data-driven business. Only through concrete implementation guidelines can the rather abstract terminology of human rights be meaningfully translated into expectations as to what has to be done, and a common understanding of the expectations towards responsible business conduct in the data economy be established. The traditional focus of such processes often looks from global North headquarters into supply chains in the global South, and deals with issues such as child labour in cocoa production, exploitative working conditions in the fishing industry or health, safety issues in textile factories or deprivation of land by the extractive industry (Baumann-Pauly & Nolan, 2016; Bernaz, 2013). The current focus on digital rights in the global North has started to spread around the globe, and there is a growing discourse as to what inclusive governance structures for digital businesses could be implemented that correspond better to cultural contexts in the global South and specific cultural-political regions (Arun, 2020; Latonero, 2018; Latonero & Kift, 2018; Mhlambi, 2020; Milan & Treré, 2019).

The right to privacy remains a cornerstone in the discussion around human rights in the digital sphere, as a growing number of rights are influenced in digital contexts (Mittelstadt et al., 2016; Reventlow, 2019; Wachter, 2018). Even though a focus on privacy in the data economy is important, a wide range of human rights beyond privacy can be affected by digital business activities. It is worth stressing that privacy issues can serve as an entry point for potential infringements of other human rights, as the data obtained through a privacy breach can reveal information that can facilitate connected human rights abuses, such as discrimination by gender or race. Privacy underpins other rights, such as rights that are based largely on collective or group activity, such as freedom of association and assembly (Bernal, 2016, p. 252). The individual's right to the safeguard of their private sphere against intrusion was first articulated in the UN Universal Declaration of Human Rights (United UN, 1948). Furthermore, the International Covenant on Civil and Political Rights elucidates in more detail the notion of privacy in Article 17 (United UN, 1966). A key reference point in particular for companies headquartered in countries that are a member of the Council of Europe is the European Convention ("Convention for the Protection of Human Rights and Fundamental Freedoms," 1950) on Human Rights (ECHR). It was adopted in 1950 and entered into force in 1953, defining privacy in Article 8 as the right to respect for private and family life, home and correspondence. The ECHR applies to states and public authorities and is not directly applicable in any manner to businesses, but it provides an important orientation for the definition of such rights with regard to companies carrying out their responsibility to protect human rights. The United Nations appointed a Special Rapporteur on the right to privacy in 2015 who defined privacy as an "enabling right" closely linked to other rights such as freedom of expression and freedom of access to information (OHCHR, 2015). Along these lines, upholding privacy can be seen as the gateway for human rights protection in the context of data disclosure requests (Ebert et al., 2020).

As more and more data is processed in the private sector, and on occasion transferred to public services, that may increasingly tap deeper into an individual's

life, the question emerges as to where the state duty to protect human rights ends and the corporate responsibility to respect human rights begins. Finding a new balance between these spheres becomes even more important when data that has been collected for “commercial” purposes in the private sector can reveal information about the data subject that can be used “against” the individual when in the hands of the state. This indicates a strong tension between the state duty to protect the data subject from privacy infringements and the responsibility of companies to respect data subjects’ very same rights. A company might collect data following a data extraction logic that aims at the maximization of data to drive revenues from improved targeted advertising; later, a government might tap that same data pool created through data maximization practices by the company (Sadowski, 2019). To disentangle the respective responsibilities of state and business towards individuals’ privacy and wider human rights impacts in that interlinked dynamic is not an easy task, and the literature has not fully addressed such dynamics from a B&HR perspective yet.

The B&HR debate has slowly started to pay attention to human rights impacts resulting from digital business activities (Ebert et al., 2020; Jørgensen, 2019). From a broader perspective, Risse and Livingston call for further research conceptualizing the impact of artificial intelligence on human rights with regard to the moral implications of a sort of “super intelligence” without value commitment (Livingston & Risse, 2019; Risse, 2019). Jørgensen explored how platforms frame human rights and which story they aim at telling, and outlined strong differences around the conceptions of privacy in Europe in comparison to the US (Jørgensen, 2017, 2018). Research shows that the discourse within US-based tech companies frames privacy as a data control issue (who has control over the data), rather than reflecting whether data minimization (reducing the collection of data to the necessary minimum) might better enable privacy protection. This logic would increase the responsibility of data subjects for the management and hence processing of their user data by giving the responsibility of privacy protection back to the user. This shifts the focus away from the actual privacy-intruding body, and puts the burden of protecting privacy on the data subject. Overall, Jørgensen retraces how certain companies’ logic centres on potential human rights violations by governments, with less emphasis placed on issues where the companies’ own business practices might adversely impact their users’ human rights (Jørgensen, 2017, p. 291). In addition, scholars have discussed the implications of social media and the internet with regard to the conduct of foreign companies in China (Jiang, 2016), how Internet Protocols could be used for the benefit of human rights (Krishnamurthy, 2019), and who would be liable for human rights harms under tort law considerations (Engelhardt, 2019).

To date, there is very sparse literature on businesses applying the B&HR lens to managing human rights risks in a datafied business environment (Ebert et al., 2020; Samway, 2016). The B&HR discourse remains nascent with regard to systematically and/or empirically exploring the human rights impacts of data-driven business practices in specific business situations, and indeed how companies are actually managing these. As the previous discussion has illustrated, these specific scenarios can become particularly complex in the state-business nexus (Pasquale, 2015): states and business have a shared interest in not revealing too many details to the public, yet might diverge with regard to their data-based inter-linkages, such as data maximization, to drive advertising revenues versus controlling their citizens

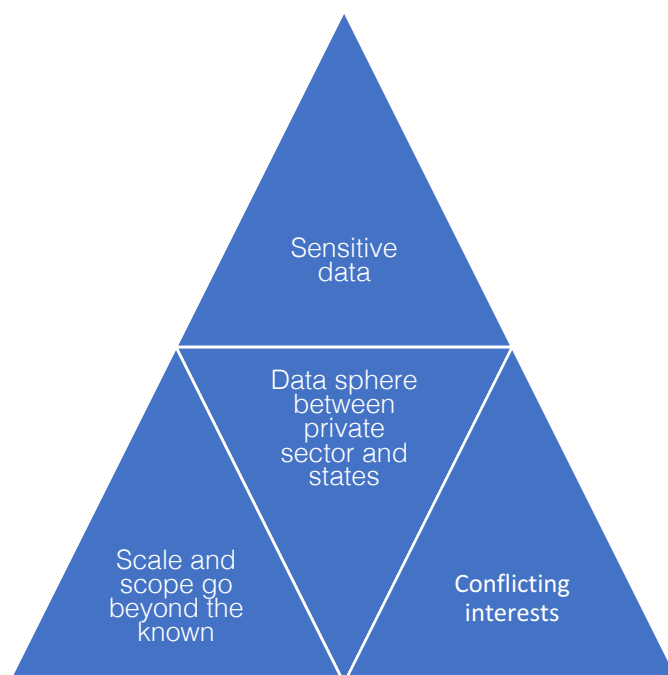


Figure 2: Data sphere between the private sector and states (own illustration)

4.2. The need to better understand the state-business nexus in the data economy

In essence, there is an extensive gap in empirical research examining how “black boxes” (Pasquale, 2015) in the data economy can be opened and assessed from a human rights-based approach. In particular, there is a need to better understand the state-business nexus, where data is power. This chapter has demonstrated that the scale and scope of data sharing between the state and private actors extends beyond what is currently acknowledged, due to the extensive penetration of data-driven business logic across a range of sectors in which business and the state cooperate. Adding to this, the data in the state-business nexus is likely to be sensitive in nature when looked at through the eyes of the rights holder. Nevertheless, this chapter has also shown that the interests of the state and business actors might be conflicting and not easy to align.

The state-business nexus on data needs to be placed in a wider debate regarding norms conflicts in internet governance and the quest to define what constitutes “good governance” of new technologies (Cath, Wachter, Mittelstadt, Taddeo, & Floridi, 2018). From one perspective, the liberal model is footed strongly in private self-regulation, soft law and discursive multi-stakeholder processes, and in emphasizing human rights, freedom of expression and a limitation of state control (Flonk, Jachtenfuchs, & Obendiek, 2020, p. 386). On the other hand, the strongly sovereign approaches spearheaded by Russia and China, supported by certain developing countries, call for a new configuration of norms and institutions that diverge from the domination of a small number of Western states and companies that have to date shaped the rules with global reach (Flonk et al., 2020). These streams see internet-based communication as a threat to domestic values and stability that require control and restriction rather than encouragement (Flonk et al., 2020, p. 386). Two current cases in the public spotlight shine further light on the continuing struggle to find an equilibrium for the data sphere between the private sector and the state. The first is the case of Hong Kong, where a recently introduced security law has raised human rights concerns and resulted in several tech companies such as Google, Twitter and Facebook deciding to halt data exchanges with the Hong Kong authorities (Hern, 2020 ; Z. Whittaker, 2020). The second is the currently pending case brought by The Gambia against Myanmar in front of the International Court of Justice, in which a claim is made that the Rohingya crisis in Myanmar constituted a planned genocide. In light of this, The Gambia has requested data from Facebook (Smith, 2020). The data requested from Facebook is alleged to provide evidence from communications by the Myanmar police and military of the intent of their actions, which amount to a systemic attempt to eradicate of a population group (Ochab, 2020). Facebook has denied the request, claiming it is too broad and that it would violate US law if the data were handed over (Smith, 2020), but the process remains on-going at the time of writing. Both cases illustrate the intricate nature of such requests and their potential diplomatic repercussions.

The aim of this research is to bring clarity to the current opacity of interaction between state and company in the data sphere, by looking at the precise case of data disclosure requests for user data as a phenomenological manifestation of a “black box” in the state-business nexus within the data economy. This area of research deals with harms to people that are not instantly felt, but the impact of which can be grave for the rights holder. Also, it is a field of practice characterized by high volatility in diplomatic tensions between home and host state. The potential quality of information is so high that a government might be very interested in obtaining data to uphold or expand its power, in particular in fragile political settings, where a particular emphasis of the research will be set.

III. The case of data disclosure requests: a black box in the state-business nexus

1. Situating the socio-political significance of data disclosure requests

Data requests from governments to tech companies are situated deeply within the state-business nexus and hinge in governance questions in the data economy. As defined in the introduction, government data requests for user data (also referred to as “metadata”) 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), and invoicing and payment information – in cyber policy commonly referred to as “new surveillance” (Bernal, 2016). The current governing frameworks that deal with data sharing practices between the private and public sector have been challenged by the expansion of the internet, communications and technology companies and their services across borders in combination with accelerating datafication. On the one hand, there are certainly well justified law enforcement requests for fighting crime and/or upholding national security. On the other hand, requests to companies for user data are prone to power abuses by governments seeking to serve other purposes. In theory, data collected in any type of business sector can be the potential object of a government data disclosure request, and the demands on big tech companies can be seen as just the tip of the iceberg. Governments request data from companies that are headquartered within the same jurisdictions, mostly nation states, as well as across jurisdictions, such as to subsidiaries or foreign corporate entities. A company might be headquartered in the country of the authority that is requesting the data, or a company might be headquartered outside of the jurisdictions of the requesting government authority.

Government requests for user data that are being judged by business actors as “unusual” (and are therefore to a certain extent “unforeseen” or “surprising” in nature) are the kinds of requests that are of interest to this work. Conflicting regulatory frameworks and conflicting organizational norms in cross-border cooperation make navigating requests an organizational tightrope fraught with plenty of political traps (e.g. a local host government for data held in the home state of the headquarter)

Research demonstrates that government requests for data disclosure, especially user data, are by no means limited to authoritarian states, or indeed states where violent conflict is imminent or manifest. These requests are widespread in liberal democracies, especially under the rhetoric of preventing terrorism (Boghosian, 2012). However, the potential effects of these requests in authoritarian states and conflict zones can have more severe consequences for affected individuals, such as the arrests and/or detentions of opposition members, and/or violent attacks in combination with little or no means of fair and transparent trial/constitutional re-dress or right to remedy (Flyverbom, Deibert, & Matten, 2019).

2. Lack of data to form an empirical basis to evaluate business conduct

Stakeholder expectations, such as those of customers and investors, have become more and more demanding towards companies: corporate management is under pressure to re-visit their business practices from a human rights-respecting angle (Flyverbom et al., 2019). Consequently, corporate actors must very carefully weigh their decisions on whether and which data to share in order to protect their users' privacy (Crawford & Schultz, 2014). Data breach scandals have led, and will continue to lead to, tremendous corporate reputation and financial damage (Solon, 2016).

In order to address these concerns, larger and mid-size tech companies are increasingly demonstrating their willingness to disclose more information about their actual conduct with governments by publishing so-called "transparency reports". While the transparency reports are supposed to shed light on the cooperation between government actors and the private sector, the extent to which they are useful in determining actual corporate behaviour is fairly limited, as for example researchers in civil society organizations (Cardozo, Cohn, Higgins, Opsahl, & Reitman, 2014) and academics have highlighted (Parsons, 2019, p. 112). Companies' track records regarding data disclosure requests and respecting privacy remains non-transparent in nature, as has been argued by computer science scholars (Parsons, 2019; Rahman, 2016; Soghoian, 2011). Scholars point out that the publicly displayed metrics regarding data requests in transparency reports are not substantively informative in nature as companies cannot report on requests in some jurisdictions and, even when they can report about them, numbers are neither comparable nor instructive. For example, it remains unclear what one unit of data requests stands for in terms of volume and quality of data requested. This is due to a lack of sufficient detail in the figures. The incommensurate nature of data across companies is due to an absence of standardization, so one unit of data disclosure requests in company A's report might stand for something completely different to a unit in company B's report. While research also shows that companies start to act on the risk of becoming complicit in potential governmental human rights abuses – such as infringements of privacy – transparency alone might not suffice to hold actors accountable for algorithmic opacity (Ananny & Crawford, 2018; MacKinnon, 2007; Samway & Ryan, 2014). Where, then, is the missing piece of this puzzle?

In a neighbouring area of research, scholars are embarking upon quantitative analysis with regard to the scale of network shutdowns and potential connections with ownership structures of internet service providers (Freyburg & Garbe, 2018). Network shutdowns have the "benefit" of being a type of government demand that is clearly noticeable to the public if the request is enforced, since access to the internet will be impaired or curtailed entirely. Due to the lack of informative empirical data, dealing with data disclosure requests is a field characterized by scarce empirical knowledge from a scholarly perspective, but can have negative impacts for users similarly as salient as the impacts of network shutdowns (Rydzak, 2018). Data disclosure requests are a more indirect approach than network shutdowns, and can be used strategically

by the government in a manner that will not be so easily sensed by the public. Government demands for user data are thus a relatively discreet way to retrieve detailed information about an individual or group of people. The affected individual(s) will not “feel” when the disclosure takes place and the public will not notice it either. What affected individuals will actually feel are the consequences of the decisions taken by governments, based on the disclosed data. Scholars have highlighted that transparency with regard to government interference in digital communications is seriously limited, partly due to gag orders under US law for example, and similar legislation in the UK on secrecy as to government cooperation on national security issues, such as the UK’s Investigatory Powers Act, (2016). Other governments around the world have shown keen interest in keeping their demands to the private sector secret (Glasius & Michaelsen, 2018; Greenwald, 2015; Howard, 2015; L. Woods, 2017). Many governments appear to have little to no incentive to encourage greater transparency from companies about data requests.

The vast knowledge gap on practice inside companies reacting to disclosure requests stands in contrast with an extensive amount of literature on government surveillance and ubiquitous data collection and analysis by the private sector (Elswah et al., 2019; Glasius & Michaelsen, 2018; Gray & Henderson, 2017; Howard, 2015; Zuboff, 2015, 2019). Dealing with government requests for data disclosure, and specifically user data, is a precarious issue for business leaders. Despite its importance, the issue is systematically understudied from a management perspective, partly due to a lack of reliable empirical data. This research therefore aims at making a contribution to closing this gap, in the next sections by drawing together different research and policy contexts to provide orientation for managerial practice in dealing with data disclosure requests, before diving into an empirical exploration of how companies manage such requests in the next chapter (IV.).

3. A managerial dilemma: data disclosure requests under a fragmented status quo

In current practice, the governance gaps in the political economy of data-driven business are carried to the state level. This dilemma raises the question as to what responsible business conduct could indeed look like in such a setting: in the case of data disclosure requests, how can the enforcement gap between the state duty to protect human rights, including in the digital space, along with the corporate responsibility to respect human rights including privacy, be closed.

3.1. A contested legal terrain: data sharing across jurisdictions

As was underscored previously, the information companies (can) disclose in the public domain with regard to their processes on dealing with data disclosure requests is limited. It remains challenging for the companies to determine the appropriate response vis-à-vis compliance with local law, and how this local law might stand in conflict with international law or the human rights responsibilities of a company (GNI, 2020a). In the following, I review the current literature as to what it says of the transatlantic data exchange framework for US and EU-based companies, and how it

is relevant for data disclosure requests as examples of global data exchanges. Of course, these are not representative of data-handling globally, yet a significant share of data worldwide is stored and processed within the US and the EU region. Additionally, companies based in the global North may be more likely to refer to a business and human rights narrative, among other factors, due to government pressures to comply with National Action Plans (see III.4.) on business and human rights in their home country (De Felice & Graf, 2015; O'Brien, Mehra, Blackwell, & Poulsen-Hansen, 2016).

Mutual Legal Assistance Treaties (MLAT) and letters rogatory/letters of request allow international evidence exchanges in criminal procedures (Umberg & Warden, 2014). Such an MLAT process can be initiated when a treaty facilitating the exchange of evidence exists and the letters rogatory process can be used when a treaty does not exist to facilitate the exchange between courts (Umberg & Warden, 2014). In the United States, MLATs are negotiated by the Department of State in cooperation with the Department of Justice, and follow a similar logic in many European states, such as the UK or Switzerland (Feng, 2007; Frei & Trechsel, 1990; A. K. Woods, 2017). MLAT may address, for example, foreign law enforcement's access to data. However, this process is lengthy and may be subject to other legal requirements, such as dual criminality, and has been criticized by certain parties as not being a very appropriate means in the digital age, while others see it as a safeguarding mechanism against foreign interference (A. K. Woods, 2017).

The relationship of data sharing between the European Union and the United States is exemplified as a contested terrain, in particular due to differing notions of privacy and freedom of expression under US and EU law (Weiss & Archick, 2016). Although the introduction of the EU General Data Protection Regulation (GDPR) continues to be seen as a major milestone for privacy rights, criticism remains as technological advancements might be able to bypass some of the mechanisms of action in the GDPR (Nouwens, Liccardi, Veale, Karger, & Kagal, 2020; Veale, Binns, & Edwards, 2018; Wachter, 2018).

In essence, data sharing practices remain opaque, in particular across borders – even where cooperative frameworks exist – because law enforcement agencies operate on different constitutional footings (A. K. Woods, 2017). Observing the lack of clarity for data sharing practices between the EU and the US, one is also aware that sharing practices of user data across other jurisdictions are also complex (A. K. Woods, 2017). In contexts in which such frameworks are absent, data sharing practices are entirely unclear. Struggles between conflicting definitions of privacy and governments interested in obtaining data from companies across jurisdictions lead to continuous uncertainty in the practice of management. In the following I explore the limits of looking at data disclosure requests from a managerial approach that centrally assesses the legal compliance dimension.

3.2. Why does a legalistic approach to data disclosure requests not suffice?

Even though government requests for user data are often discussed from a legal angle, there are reasons why purely legal approaches cannot fully shed light on the dynamics inside a company. Firstly, legal processes might not serve as the right avenue for addressing ethical issues arising from privacy or broader human rights issues across borders, where local contextuality is key (Milan & Treré, 2019). 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 standard for corporate behaviour in line with B&HR. Secondly, the leverage governments can exert in many host or home states on companies, sometimes with the use of force and/or physical violence to persons, might render the legal process quite weak and/or arbitrary, according to government goodwill. If staff are threatened or data servers are seized when a company does not comply with a data disclosure request, a cross-border legal compliance processes is deemed to be ineffective (Parsons, 2019). Hence, from the perspective of a corporate manager who finds themselves in a dilemma of conflicting laws and interests, a more practice-oriented angle is necessary to deal with data disclosure requests. Thirdly, some of the internet, communications and technology companies that are subject to data disclosure requests are powerful players that can lobby and partly set or influence the agenda on disclosure requests and might follow a set of company values when doing so (Moore & Tambini, 2018; Webb, 2019).

In summary, data disclosure requests from governments to companies make a compelling case for analyzing management practices within the fragmented governance of human rights. In order to better understand in which current policy context the company management operates, key elements of the policy developments which attempt to govern the gap will now be outlined.

4. Policy context: governing the gap?

In the context of the debate around the human rights obligations between states and non-state actors, this section will sketch the different tools and guidance emerging at the supranational and national level (4.1), in multi-stakeholder-initiatives and from civil society organizations (4.2.) that companies can use to form a better understanding of the phenomenon of data disclosure requests and adjust practice in a rights respecting way, to circumvent or close persisting loopholes (4.3.) and ultimately address a microcosm of the global governance gap through thick stakeholder consensus (4.4.).

Persisting loopholes have to be seen in the policy context of the tensions between the state duty to protect human rights and how business plays into it. Several initiatives at the UN level aimed at more clearly deliniating the role of the company under international human rights law more clearly have been initiated, but with little success. Among the failed attempts to anchor the societal responsibilities of business in the human rights framework were the United Nations Sub-Commission on the Promotion and Protection of Human Rights' "Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights" (Kinley,

Nolan, & Zerial, 2007; Weissbrodt & Kruger, 2003). A strategic stakeholder engagement process from 2005-2008 led to success and resulted in the adoption of the UN Guiding Principles on Business and Human Rights (UNGPs) by the UN Human Rights Council in June 2011 (Ruggie, 2007, 2013). This framework has since become a key reference for rights-respecting management in global governance, and policy-makers are working on demonstrating its relevance for the digital realm.

4.1. Rights-respecting management based on the UNGPs

In his role as the UN Special Representative of the Secretary-General on human rights and transnational corporations and other business enterprises, John Ruggie led a global consultation process with relevant stakeholders (governments, business, civil society, trade unions, academics) that resulted in the Protect, Respect, Remedy Framework (Ruggie, 2007, 2013) and the later adoption of the UNGPs (compare II.4.).

A new workstream might also deliver important insights on policy around internet, communications and technology companies' responsibilities to uphold human rights with regard to data, also in light of data disclosure requests. In 2019, the Office of the High Commissioner for Human Rights (OHCHR) announced a new project on Business and Human Rights in Technology (B-Tech) (OHCHR, 2019). The project sets out to provide authoritative guidance and resources to enhance the quality of implementation of the UNGPs with respect to a selected number of strategic focus areas in the technology space (OHCHR, 2019).

Of note, while the UNGPs are primarily a soft-law instrument, major parts of the state duty to protect are enshrined in international human rights law (compare II.4.). With the foundation in the UDHR combined with more practical guidance, the UNGPs also set out that states should implement the UNGPs at the national level, through a smart mix of regulatory and voluntary initiatives and incentives in the format of a National Action Plan on Business and Human Rights (NAP) (Baumann-Pauly & Nolan, 2016; O'Brien et al., 2016; UN, 2011). Moreover, since the UNGPs cover all businesses in all sectors, this means that in principle, internet, communications and technology companies also have the responsibility to respect human rights. In practice, however, the UNGPs have been understood to place an emphasis on sectors with human rights issues within supply chains, such as the manufacturing conditions of hardware devices. Yet, the business and human rights community increasingly recognizes that the effects of the actual technological products and their data collection (devices, but also growingly digital products and services) needs to be included in such NAPs as well (Ebert et al., 2020). The Danish Institute for Human Rights, for instance, recently issued guidance on how the tech sector can be addressed in NAPs (Wingfield, Tuta, & Bansal, 2020).

The UNGPs offer guidance on how business ought to implement their responsibility to respect human rights in their business operations. The process to establish a systematic handling of human rights inside the company is referred to as "Human Rights Due Diligence" (HRDD) (UN Human RightsUN, 2011) and could in theory give

further insight as to how business enterprises could also assess their human rights impacts in a data-driven environment. HRDD should assist businesses in operationalizing their human rights responsibilities in a manner that can be mainstreamed across all business units. HRDD builds upon a thorough Human Rights Impact Assessment (HRIA) (UN Human Rights, Götzmann, 2019; UN, 2011). This assessment forms part of a due diligence process that is not static in nature. The UNGPs do not require that businesses conduct human rights impact assessments by using that exact terminology, but they indicate approaches that equal essential elements of a human rights impact assessment (Götzmann, 2019). HRDD is often comprised of a four or five step model to identify and address potential and actual adverse impacts on human rights, and mitigate human rights issues arising from a business's activities, embedded at the appropriate level (Götzmann, 2019). This includes drawing on internal and/or independent human rights expertise, and undertaking meaningful consultation with potentially affected rights holders and other relevant parties (Götzmann, 2019). Gender-sensitive language and a particular focus on any human rights impacts on individuals belonging to groups that may be at heightened risk of vulnerability or marginalization are commonly stressed (Awori, Anumo, Montes, & Hughes, 2018). It is important to carry out the assessment of impacts from the perspective of risk to people rather than risk to business, as well as repeating risk and impact identification and assessment at regular intervals (Götzmann, 2017, 2019).

Developed by the Electronic Frontier Foundation in cooperation with several experts under the auspices of the UN Human Rights Council, the Necessary & Proportionate Principles (EFF, 2014) offer further guidance for rights-respecting practices in communications surveillance, applicable “regardless of the purpose for the surveillance – including enforcing law, protecting national security, gathering intelligence, or another governmental function (...) both to the State’s obligation to respect and fulfill individuals’ human rights, and also to the obligation to protect individuals’ human rights from abuse by non-State actors, including business enterprises” (EFF, 2014). Given their key role in designing, developing, and disseminating technologies, enabling and providing communications, and in facilitating certain state surveillance activities, business enterprises are specifically included in the Necessary & Proportionate Principles with their responsibility for respecting individual privacy and other human rights. The principles highlight the importance of legality, necessity and proportionality as an analytical grid required by International Human Rights Law.

4.2. Multi-stakeholder efforts on human rights in data-driven business

As a result, from the cases emerging in the early 2000s, such as the one that involved Yahoo! in 2005 (see chapter II.2), various stakeholders came together, agreeing that the governance gap between corporate practices, and international and human rights laws and norms – in particular regarding freedom of expression and privacy in the tech sector – posed a challenge that needed to be addressed in a systematic way (Samway, 2016; Samway & Ryan, 2014). In 2008, the Global Network Initiative (GNI) was founded by Google, Microsoft and Yahoo!. Since its early days, it has emerged

as a multi-stakeholder organization with significant business buy-in that can mount a collective response to the joint challenges of internet governance (Maclay, 2010). Member companies today include Facebook, Google, Microsoft and Yahoo!, along with other member organizations from civil society, socially responsible investors, academia and individual experts (Maclay, 2010). In 2011, the Telecommunications Industry Dialogue (TID) was founded and extended the geographical scope of their member companies from the US to include Europe (Nokia, Millicom, Orange, Telenor, Telefónica, Telia Company, Vodafone) and published their Guiding Principles on Freedom of Expression and Privacy (TDI, 2019), aligned with the UNGPs (Samway, 2016). Seven global telecommunication companies from the TDI merged with the GNI in 2017, thereby also extending the geographical scope of the GNI from a rather US-centric organization to a broader network which included leading European companies (Millicom, Nokia, Orange, Telefónica, Telenor Group, Telia Company, and Vodafone Group). GNI's membership base is constantly growing, with efforts to improve geographical diversity ongoing – South Korean company LINE has joined (Global Network GNI, 2020b). This in the past was one of the key criticisms leveled at the network (Maclay, 2010).

The “GNI principles” were defined in negotiations between GNI members in 2008 (Global Network GNI, 2017). These principles lay out the initiative's foundation with reference to key international laws and norms including the Universal Declaration of Human Rights, the Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights. The principles received an update in 2017 which specifically references two international instruments published after the GNI Principles were launched in 2008: the UNGPs published in 2011, and the 2011 updated version of the OECD Guidelines for Multi-National Enterprises (Global Network GNI, 2017).

In addition to these principles, the GNI set up the so-called “Implementation Guidelines” covering five sets of obligations for companies to comply with: freedom of expression, privacy, responsible company decision-making, multi-stakeholder collaboration and governance, accountability and transparency (Global Network GNI, 2017). GNI member companies' implementations of the Principles and Implementation Guidelines are assessed on a biannual basis and are documented in assessment reports after each assessment cycle, including anonymized information in combination with some selected, attributed information. In 2016, the NYU Stern Center for Human Rights and Business withdrew its GNI membership stating that the development of a credible system for evaluating company compliance with human rights standards had failed, and that the current company assessment procedures were not sufficiently transparent in nature (Labowitz, 2016). The debate continues as to how best to provide better transparency and implementation within the GNI. Nevertheless, the latest GNI company assessment report for the cycle 2018/2019 (GNI, 2020a, p. 17) highlighted how certain telecommunications companies and platforms continue to operate in difficult environments. Certain companies aim at jointly working on issues regarding questionable government requests (GNI, 2020a), under the auspices of the GNI, but with very little information about concrete decision-making or red lines being made available in the public domain. In its concluding

recommendations on the 2018/2019 company assessment cycle (GNI, 2020a, p. 96f) the GNI acknowledges the ongoing challenges around state surveillance, stating that “legal prohibitions on the disclosure of information related to national security requests and concerns for safety of local personnel continue to be a legitimate obstacle to companies’ ability to be transparent about these requests”.

Civil society organizations such as Ranking Digital Rights (RDR) (Maréchal, 2015; RDR, 2020b), Access Now (Access AccessNow, 2018) and the Electronic Frontier Foundation (EFF) (Blumberg & Eckersley, 2009; EFF, 2020) all conduct important work with the goal of holding the tech sector to account for adverse impacts on human rights, which includes several workstreams that are relevant for the B&HR agenda. One of the most relevant civil society information sources for shedding light on data sharing practices between the private and the public sector is the benchmark produced by RDR. The RDR benchmark is a yearly benchmark of market leaders in the tech sector based on their publicly available policies and documents about data governance, freedom of expression and privacy. Besides empowering activists to hold technology companies to account, the aim of RDR is to create transparency for users to make better informed choices, provide information to investors for due diligence and investing decisions and enhance media reporting on transparency efforts in the sector.

4.3. Persisting loopholes in legal frameworks

Looking at data disclosure requests from applied practice, the process appears to be characterized by formidable loopholes , as data disclosure requests require large degrees of interpretation. MLATs do not exist between all companies and tend to be used primarily for content requests, since most telecommunications companies are required to store location/user data locally, and in any case provide it upon request as a condition of their license. (Unlike in the case of content, there are no significant blocking statutes for metadata.) There are also multilateral mechanisms for facilitating investigative data across borders, e.g. the Budapest Convention/CoE 24/7 network (Council of Europe, 2001) and/or mechanisms such as the CLOUD Act (US Congress, 2018) and the proposed EU E-evidence regulation (E.U. Commission, 2019) which may further modify cross-border law enforcement’s access to data. The MLAT process takes significantly more time than the domestic law enforcement process for requesting data (through the Stored Communications Act, codified at 18 U.S.C. Chapter 121 §§ 2701–2712) and such a time lag might be an annoyance and an actual impediment to requesting government bodies. Adding to this, recent case law has shone light on how data sharing between the European Union and the United States has changed significantly since the Court of Justice of the European Union (CJEU) scrapped the “Safe Harbour” agreement in the Max Schrems case in 2015 (“Case C-362/14, Maximilian Schrems v Data Protection Commissioner,” 2015; Weiss & Archick, 2016). The court ruled that the interference in fundamental rights is contrary to the principle of proportionality due to the large-scale, indiscriminate surveillance carried out by the United States intelligence services (“Case C-362/14, Maximilian Schrems v Data Protection Commissioner,” 2015; Weiss & Archick, 2016). The EU-US Privacy Shield Framework substituted the Safe Harbour agreement (Weiss & Archick,

2016). Subsequently, the EU General Data Protection Regulation (GDPR) entered into force in 2018 (European Commission, 2016), aiming at the protection of all EU citizens from privacy breaches. Its main features are increased territorial scope, penalties (up to 4% of annual global turnover or €20 million), consent, and a range of data subject rights. The extension of territorial scope means that the GDPR is applicable to every company that processes the personal data of data subjects residing in the EU, regardless of the company's location. The request for consent must be presented in an easily legible, clear, distinguishable format, with the purpose for data processing attached to that consent. That consent might be withdrawn must be an option. The data subject has particular rights, such as the right to be notified in case of a data breach, the right to access his or her data, the right to be forgotten (data erasure) along with data portability across platforms/service providers. Also, technical and organizational measures have to be implemented in an appropriate and effective way to assure privacy by design. There is an extensive back and forth with respect to transatlantic exchanges of corporate data between states; they follow predominantly the same values and understanding on human rights, yet are distinct with regard to privacy. In the course of writing this research, in July 2020, the CJEU overruled the EU-US Privacy Shield framework for data exchanges between the European Union and the US, again based on a case brought forward by Max Schrems on behalf of None of Your Business (NOYB), judging it as unlawful on the basis of standard contractual agreement (CJEU "Case C-311/18," 2020; None of Your NOYB, 2020). The longer-term impact of this judgement on the legal framework at the time of writing remains to be seen.

It is worth highlighting that there are many jurisdictions across the globe in which governments do not necessarily follow constitutional provisions, or do not necessarily show sufficient respect to the right to privacy, or where there is no legal framework for regulating the obtention of user data, and/or where governments may use "authoritarian practices" such as violent threats to obtain user data from companies (Glasius & Michaelsen, 2018).

4.4. Data disclosure requests as a microcosm of digital global governance

Investigating the current state of business responses to data disclosure requests from a human rights perspective appears as a "microcosm of a larger crisis in contemporary governance" (Ruggie, 2014, p. 6). The case of transnational, unconventional data disclosure requests demonstrates that the old governance model has only limited capacity to deal with significant global challenges in a solely top-down, hierarchic manner. Outdated frameworks for cross-border data access requests from governments to companies are so slow and unfit for purpose that governments aim at finding other ways to get to the data they want; through this, governments might cause unnecessary harm to the individuals affected. Rather, the case of data disclosure requests might require new governance models following a "building blocks approach" (Ruggie, 2014, p. 8) for co-developing different elements to find solutions and embed them within an international political framework. The concept of "thick stakeholder consensus" describes an emerging code of good practice for developing standards or new forms of cooperation outside international

law, which is normatively thicker as it is proven to be more inclusive, transparent, and predictable (Pauwelyn, Wessel, & Wouters, 2014, p. 749). Thick stakeholder consensus can also rely on more diverse and higher-level expertise, and through that provide a more careful and coherently elaborated output for norm development. Yet, to empower stakeholders to create a more effective normative framework, we first have to better understand how business currently aims at managing data disclosure requests from governments, using the opportunities and dealing with the challenges that have been sketched in this section on the policy context.

In summary, data disclosure requests from governments to companies are an interesting case to explore the manifestation of black boxes in the data economy, both in the context of a specific case and from a human rights approach. Firstly, they are characterized by a striking opacity of interaction between the state and the company. Secondly, as with many harms occurring in the data economy, the harm is not instantly felt even when impacts are adverse but only experienced at a later juncture. Thirdly, the implications can be especially volatile for diplomatic tensions between home and host state and disrupt normative understandings of global governance. And last but not least, the quality of information that can be obtained is so high that governments will often be very keen to tap into that data. Combining all these elements, a government's motivation to creatively apply force might be considerably high.

In practice, the business activities, products, and services of technology companies can contribute to escalating or exacerbating conflict in connection with government action. Surveillance of personal data or metadata by conflict parties can also render people more vulnerable and expose them to a heightened risk of human rights abuses, for example human rights defenders and/or ethnic, racial or religious minorities. Governing such data in conflict zones or crisis situations poses heightened risks to rights holders. It therefore needs to be taken into account what harm can result when technology companies share data with conflicting parties.

The following chapter outlines a methodological approach and proposes sensemaking as the conceptual framework employed to investigate the hidden and invisible processes of companies' responses to government data disclosure requests.

IV. Exploring the black box: making sense of data disclosure requests

This chapter aims at opening a specific “black box” in the data economy by looking at how companies make sense of data disclosure requests through a qualitative research design. It lays out the methodological considerations, data collection methods by data triangulation of policy documents and expert interviews, and the sampling strategy for the expert interviews. The data analysis presents the patterns of the corporate response to data disclosure requests.

Chapter II. has highlighted that there is an extensive gap in academic literature examining rights-respecting digital business practices in specific situations. Adding to this, as Chapter III. has also demonstrated, there is a lack of empirical data as to the actual volume of requests. Beyond the notion that transparency reports do not provide sufficiently high-quality information, little information is available in the public policy domain on the actual handling by companies of data requests from governments. Given the combination of nascent academic discourse with sparse insights in the public domain, the clues that can be drawn from actual company practice by researching inside corporate entities can deliver important insights into the actual dynamics at hand: how do companies respond to user data requests from governments? The research should grasp in-depth information and furnish nuanced data on company context, meanings and processes. The importance also ascribed to the resources that companies allocate in corporate governance to developing coping mechanisms for dealing with such requests might also give an indication as to the scale of the phenomenon, along with the dynamics amongst the employees responsible. It requires a qualitative research design to better understand the dynamics at hand (Miles & Huberman, 1994; Strauss, 1987).

As the field is characterized by little empirical knowledge from a scholarly perspective (Goethals, 2019; Obara, 2017), new themes and directions are likely to emerge inductively (Strauss, 1987). The conceptual framework below builds on a sensemaking theory (Weick 1995) and explains the main elements to be studied to explore how companies respond to data disclosure requests (Miles & Huberman, 1994, p. 18): corporate policies and practices such as the internal process of exchange about requests, and external consultation with stakeholders, and reveal the main themes of interest as elements of response when a government request for user data comes in.

As this research is connected to the discourse on business responsibilities towards human rights protection, the dimension of human rights due diligence or privacy safeguards are added as a specific element of interest for the research community. In sum, information gathered from emerging themes of the collective response at the organizational level will provide insights on how companies react to data requests. It should allow for the description of different corporate approaches to deal with such requests and the identification of similarities and differences in response patterns.

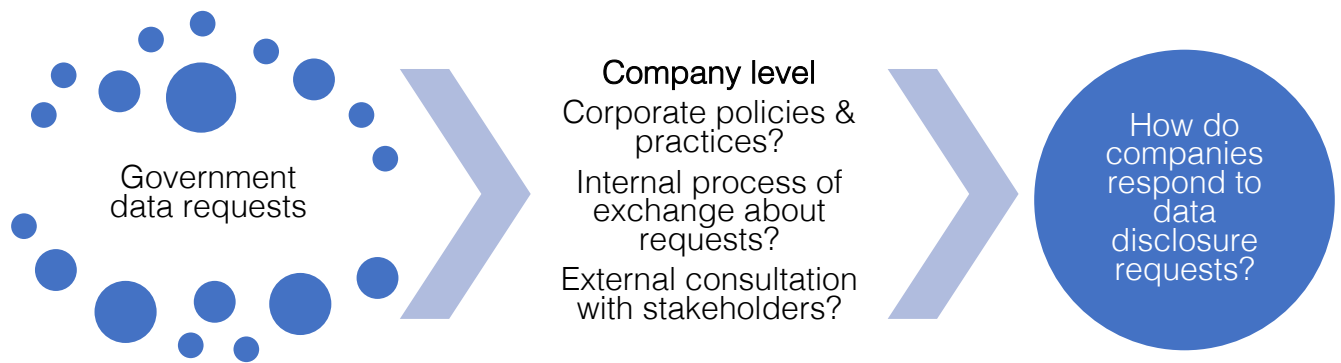


Figure 3: Frame of analysis (own illustration)

The ontology and epistemology underlying this qualitative research design and choice of sensemaking theory follows a constructivist logic. Sensemaking is the preferred framework here as it can, on the one hand, cover catastrophic or utterly unanticipated outcomes and, although there can be a range of responses, sensemaking seems primarily a type of triage tool for contingencies. In addition, sensemaking can also cover processes in “routine” situations. Government requests for data might come in the context of a catastrophe or through normal channels and with some predictability in their process.

1. Sensemaking in organizations

Sensemaking is an ongoing process to create order and make sense of what occurs (Weick, 1988, 1995, 2010; Weick & Sutcliffe, 2001; Weick et al., 2005). It allows actors to deal with ambiguity and uncertainty by creating rational accounts of the world that enable action. Sensemaking precedes decision-making and follows it by clarifying questions and answers in a social constructing process. Research shows that sensemaking can be triggered at several points in an unfolding crisis moment when actors consider the significance of disparate cues, and might encounter further cues, often generated through their own action and/or inaction which prompt them “to ask what is going on” (Maitlis & Christianson, 2014, p. 72).

A sensemaking approach (Maitlis, 2005; Maitlis & Christianson, 2014; Maitlis & Sonenshein, 2010; Weick, 1988; 1995, p. 311; 2010; Weick & Sutcliffe, 2001; Weick et al., 2005) appears as a suitable fit to give shape to emerging dimensions for the following four key reasons: (1) The appropriate level of analysis should be placed on the organizational level. It is the corporate organizational structure as a whole that responds to the external trigger of a data disclosure request. At the same time, it is a collective action of a group of individuals, in which personal actions in sum determine the trajectory of a received request. Sensemaking occurs in organizations when members confront events, issues, and actions that are to a certain extent surprising and confusing (Maitlis & Christianson, 2014, p. 64). The focus is on the organizational activity as a collective, and sensemaking is internalized by organizational members as a representation of collective action. (2) It enables analysis of interactions between a group of individuals that leads to a collective form of making sense of a situation.

To get an understanding of the organizational response to a government data request inside a company, we need to look at the collective response of a group of individuals, most likely the department responsible for dealing with the requests. This entails, for instance, inquiring about the policies, practices and strategies that are used to deal with the request or the internal process of exchange about the requests. For example, how are chains of command and reporting routines within the organization structured? Who speaks to whom, and why? Sensemaking can grasp the nuances of these human interactions. (3) It is also important to find out what are the characteristics of the decision-making process and whether the company engages with any external stakeholders or advisers on the matter. Sensemaking allows light to be shed on whether these topics emerge inductively, or whether people in fact do not frame data disclosure requests as a human rights issue (Obara, 2017). (4) The element of surprise in the literature on sensemaking emphasizes organizational hesitancy and fumbling, which naturally emerges in the response of any large organization to the unknown.

Interestingly, Karl Weick (1988) initially developed the sensemaking concept in the aftermath of the Bhopal Chemical disaster, which is also a commonly used example of business neglect causing human rights violations and connects well to the B&HR discourse (Deva, 2016; Upendra, 2016). The incident at the Union Carbide pesticide plant in Bhopal was a major industrial disaster caused by a gas leak in December 1984 in the Madhya Pradesh region of India, which resulted in the deaths of thousands (estimates range between around 2,300 to 16,000) and injured around 558,000 people. For Weick, the most interesting revelation was that there had apparently been a number of sufficiently trained staff on the ground to detect the gas leak, but who failed to do so for various reasons. He developed the sensemaking approach in light of that case study to detect why organizations respond in the way they do to unforeseen events and how sensemaking can help with understanding critical junctures. The unforeseen character relates to the exact shape and nature of data disclosure requests, not the fact that they exist per se.

The sensemaking approach in times of crisis in organization studies is still predominantly referenced with regard to the works of Weick (Weick, 1988, 1995, 2010; Weick & Sutcliffe, 2001; Weick et al., 2005) and has been subsequently further elaborated by Maitlis (2005); Maitlis and Christianson (2014); Maitlis and Sonenshein (2010). It is noteworthy that Weick stresses the importance of action as an integral part of sensemaking, stating that “cognition lies in the path of action. Action precedes cognition and focuses cognition” (Weick, 1988, p. 307). Through testing provisional understandings, action and cognition are recursively linked and actions shape the environment for sensemaking. The actions that people take in organizations produce structures, constraints and opportunities that were not there before these actions were taken (Weick, 1988, p. 306).

In the context of crisis, a situation may unfold in a hazardous and rapid manner that enables people only a slight glimpse of the information that might be required to make a fully rational decision (Maitlis & Christianson, 2014, p. 85). It is possible that individuals have a complete grasp of the information, yet they might still make

irrational decisions. Individuals do not necessarily make rational decisions and might lack information due to concurring institutional logics or personal beliefs. Hence a crisis situation might require people to take action with incomplete information.

The sensemaking literature understands the following three dimensions as important for shaping the unfolding of events (Weick et al., 2005), which will later on be taken up in the data analysis:

- Organizational factors and structures before the crisis: How much agency do actors have? How interdependent and differentiated are the roles that exist in the organization?
- Shared understanding in the organization: How do individuals hold different pieces of information? Are they able to collectively construct a new meaning? Are goals diverse?
- Early actions taken in a crisis: How do early actions determine the trajectory of the crisis? Inaction as the absence of action can have as much influence as action here. The more public and irrevocable actions are, the more justifications they require.

Weick emphasizes that people tend to think by acting (1988); hence the context of action shapes thinking (Weick, 2010, p. 547). In ethical dilemma situations, doubt plays a crucial role. Doubt can work as a stimulus that makes individuals opt for safe and best-scenario type options; organized dealing with doubt might entail sense-discrediting alongside sensemaking processes (Weick, 2010, p. 548), rendering sensemaking hesitant and leading to blunders.

Nevertheless, sensemaking might lead to a more institutionalized way of reacting to events. Sensegiving is the “process of attempting to influence the sensemaking and meaning construction of others toward a preferred redefinition of organizational reality” (Gioia & Chittipeddi, 1991, p. 442). It targets the framing of strategic change and is disseminated to an organization’s constituents (Fiss & Zajac, 2006, p. 1173). This is often accompanied by “a redefinition of the organization’s mission and purpose or a substantial shift in overall priorities and goals” (Gioia, Thomas, Clark, & Chittipeddi, 1994, p. 364). Reordering priorities might disrupt established organizational relationships and might be controversial, so it often triggers a justification process (Fiss & Zajac, 2006, p. 1174).

Maitlis and Christianson (2014, p. 98) highlight the need for more research on the question of how macro-social structures influence sensemaking in organizations, by analysing “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”. Obara and Peattie (2017; 2018) are among the first to apply the sensemaking approach in the field of B&HR. Based on interviews with managers and directors, the two scholars emphasize that B&HR scholars have developed a rationale for business responsibilities towards human rights, yet this rationale tends to remain mostly theoretical and normative, with little insight into how companies actually make sense of and use human rights inside the company (Obara & Peattie, 2018, p. 781). Goethals (2019) focused on meaning making and framing

both related to sensemaking at all organizational levels, notably employees. Adding to this, the sensemaking approach allows for more visibility in how the B&HR debate impacts companies' internal dynamics than an approach relying solely on external documents such as published company policies, reports or impact assessments (Obara & Peattie, 2018, p. 782). Applying the sensemaking approach to the interview data will make a contribution to the use of sensemaking in the field of B&HR by shedding light on the ways in which an organization makes sense of a crisis moment, when under strong political pressure and potentially confronted with salient harm to staff, customers and other affected rights holders, while highlighting what the role of human rights is in this process in companies. The research will also make a contribution to the broader literature of sensemaking in crisis with regard to analyzing which forces shape what groups notice and how they act, as proposed by Maitlis and Christianson (2014, p. 98). Hence sensemaking is a natural fit for identifying the diversion from “routine” request response to the response to “unusual” requests, and ascertaining how a company escalates those requests in deviation from the “normal”.

2. Data collection

Through the research process, the data gathered will touch upon corporate policies and practices to address data disclosure requests – such as the internal management response to requests – and the dynamics that emerge when companies consult with external stakeholders about data disclosure requests. The sources for the sensemaking consist of a review of publicly available company policies, and interviews with business representatives (company representatives, business associations, lawyers, consultants) as well as external stakeholders (civil society and academics working closely with industry), to ensure data triangulation.

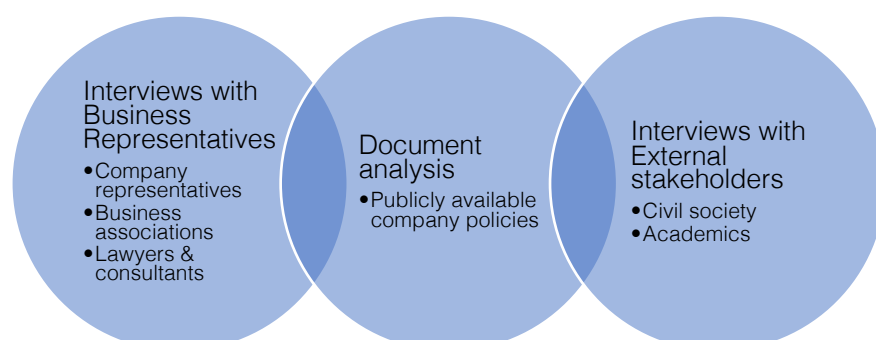


Table 2: Data sources - triangulation (own illustration)

The document analysis serves the additional purpose of preparing the researcher for an informed discussion for the expert interviews. The research design allows for a deliberately open and overarching design template for social inquiry, which can be filled with a triangulation of data sources. In order to ensure heightened confidence in the validity of the findings “the meanings emerging from the data have to be tested for their plausibility, their sturdiness, their ‘confirmability’ – that is, their validity” (Miles and Huberman, 1994, p. 11). The trustworthiness derives from rich insights drawn

from rich data sources. In order to assess the credibility of the findings with regard to plausibility and authenticity through “member reflections” (Tracy, 2010), a roundtable to engage with company representatives on the research findings had been scheduled to take place in March 2020, but had to be cancelled due to the accelerating spread of the COVID-19 pandemic. It could not realistically take place until after the submission of this thesis. Instead, the interviewed experts received a draft version of the empirical analysis for verification of the results to enhance credibility (Tracy, 2010). These member reflections helped to assess whether members find the research comprehensible and meaningful by allowing the participants to react, agree, or find problems with the research (Tracy, 2010, p. 844). The comments from the member reflections were taken into consideration in an iterative manner for enhancing the reliability of the findings.

2.1. Document analysis

Dealing with data disclosure requests in the age of decentralized internet governance is an emerging field of research. At the same time, the previous chapters have shown that, from a research perspective, the field is characterized by major constraints on publicly available documents: information on the exact nature of user data requests from government actors to companies is not reported upon in a very informative manner. Scholars repeatedly stress that corporate transparency reports do not provide the actual kind of data required, nor information on the size and granularity of the datasets (see chapter III. 3.), partly because reporting is prohibited in many jurisdictions. Also, companies do not use the same metrics to report on data requests, so the information provided is not comparable across companies (see chapter III. 3.). Adding to this, national legislation in quite a significant number of countries prohibits companies from reporting on these requests at all, or otherwise gives quite limiting requirements as to what can be reported (see examples in chapter I. and chapter III.). This results in an extensive lack of quantitative data on the actual global patterns of government data requests to the private sector, and this is why a quantitative analysis will not deliver meaningful results. The document analysis consists of a qualitative review of publicly available policies of GNI member companies on cooperation with law enforcement agencies and data sharing in broader terms. GNI member companies were chosen due to their public commitment to improve transparency in this area. For reasons of confidentiality, the sample of the document analysis is not congruent with the sample of interviewed companies as congruency would make the interview partners more easily identifiable. One should note that a qualitative document analysis that consists of reviewing publicly available company policies alone risks reproducing the assessment pointing towards opaque policies, as is claimed by several civil society organizations and think-tanks and described in chapter III. Nevertheless, the exercise can still form an important basis for engaging in an informed manner with experts in interview settings and connect those experts' statements with the discourse in publicly available policy documents.

2.2. Expert interviews

The corporate sensemaking on data disclosure requests was research based on interviews with experts in the telecommunication and internet industry. The aim of the interviews was to explore how organizational members make sense of data disclosure requests from governments, with an emphasis on unusual requests (Weick et al., 2005). To this end, I kept the interviews deliberately open, while ensuring information was gathered on four major themes. First, I inquired as to (1) governance structures for dealing with disclosure requests. Secondly, I targeted how (2) management processes an incoming request. Thirdly, a focus was placed on (3) the involvement of external stakeholders in the response process. Finally, I requested information pertaining to (4) communications and the relationship with the requesting authority. There was dedicated space given to let additional information emerge inductively, too (Strauss, 1987). The interviews were semi-structured 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 meanings inside the company and the pre-written processes involved (Obara & Peattie, 2018, p. 784). The interviews consisted of in-depth conversations of about 45-60 minutes, though on occasion they exceeded 90 minutes in length, and were slightly adapted over the course of my fieldwork. The interview structure opened with a storytelling stimulus, namely about the interviewee’s most recent, most memorable or most emblematic data disclosure case, which helped to get the conversation flowing.

2.2.1. Sampling & selection of experts

The focus of the research is on the telecommunications and platforms industry as they have historically had a high exposure to government data requests and continue to receive such solicitations. The appetite of governments to contact these companies is certainly due to their possession of extensive databases and positions as dominant market players of significant size. Additionally, the very nature of their core business activities is based on cross-border data collection, processing and analysis. This is the core business of the platform industry but not so much for the traditional telecommunications industry. Thus, the data collected reflects issues of jurisdiction related to those data flows. These data-related transactions allow for an examination of issues arising from conflicting regulatory frameworks across jurisdictions, which also potentially conflict with corporate norms, policies and practices. Also, the contractual relationship between government and telecommunications companies – which need a license to operate in a country – and to a lesser extent, platforms, makes this industry an interesting case.

This implies that the findings will primarily stand for dynamics found within multinational corporations of a certain size. Smaller companies might not be able to allocate similar resources to the matter, but might learn from particular applied strategies, or work jointly with competitors. At the same time, smaller data-driven companies have smaller data repositories than the larger multinationals, and hence might be less interesting for the government to tap into.

The sampling of the companies and their representatives were selected based on a combination of sampling strategies (Miles & Huberman, 1994, p. 28). Firstly, politically important cases that attract a desirable attention. Secondly, critical cases that permit logical generalization and maximize the application of information to other cases. Thirdly, extreme and deviant cases were chosen (as identified by the informant) to allow for information richness and learning from highly unusual manifestations of the phenomenon of interest. Regarding the first strategy, companies were chosen based on their market-size, and either hints in the public domain (press/media) that they are in a position to speak about their process of responding to data disclosure requests, or having actually shown commitment to increase transparency on privacy issues related to government requests for user data (politically important cases). For the second strategy, coverage in expert news outlets over the most recent decade pointed to a set of companies that were among the first to deal with these issues (critical cases). For the third strategy, historic experiences of company representatives with extreme cases were identified by the informant, affording the possibility of reflecting on what has changed over the course of the years, e.g. since the adoption of the UNGPs or through working together with other companies in the GNI.

Interview partners within the company were selected in accordance with whether they can speak about cases that are deemed particularly suitable for illuminating relationships and identifying the logic among corporate structures. This required speaking to key actors working within the telecommunications and internet industry. The corporate experts were selected based on their professional experiences working on data disclosure requests inside their company or in the course of their career. Most companies have designated representatives for working on these requests. Globally, this constitutes a very small set of people, and I was directed toward these representatives.

To summarise, I contacted the major players in the telecommunications and platform industry by following the three sampling strategies above and was put in touch with the appropriate representatives. Non-corporate experts were chosen due to their exposure to the topic of data disclosure requests as part of their work portfolio. These can be civil society experts working with affected individuals or political interest groups, or consultants advising corporate clients on these matters, or lawyers involved in legal action around data disclosure by companies to government authorities (defendants or plaintiffs). To a certain extent, this follows the underlying logic that the evolving narrative on data disclosure requests will be pre-determined by those who have the power to shape the discourse. The aim was also to learn of a range of past data disclosure requests that experts have dealt with, and their standard procedures, should they exist. Hence, when talking to experts the target was to discuss revelatory cases (Yin, 2013).

A total of 30 expert interviews were conducted, with a gender-balanced sample (see table 3 & 4). Twenty of these interviews were conducted with experts working inside the industry, such as company representatives, business association representatives, consultants and lawyers. Ten of the experts were academics or civil society

advocates working closely as external stakeholders or advisory bodies with the telecommunications and internet industry. From a statistical point of view, the total population of people globally designated to work on those issues inside companies is relatively small. Out of this total population, the chosen sample size in combination with iterative engagement along the respective research stages appeared as a

sufficiently supportive basis for an explorative qualitative study in such a highly politicized field of research. The company representatives willing to speak (around 2 of 10 identified) were predominantly located in the global North, whilst still having significant business in the global South, and a significant market share in many of the markets they are operating in (see also section on access to the field). I reached out to around ten companies in the global South, but they did not respond (see also 2.2.2.). Still, I was able to include a handful of external stakeholders from the global South, with some of them currently being located for professional reasons in the global North, which allows for a more balanced representation of voices.

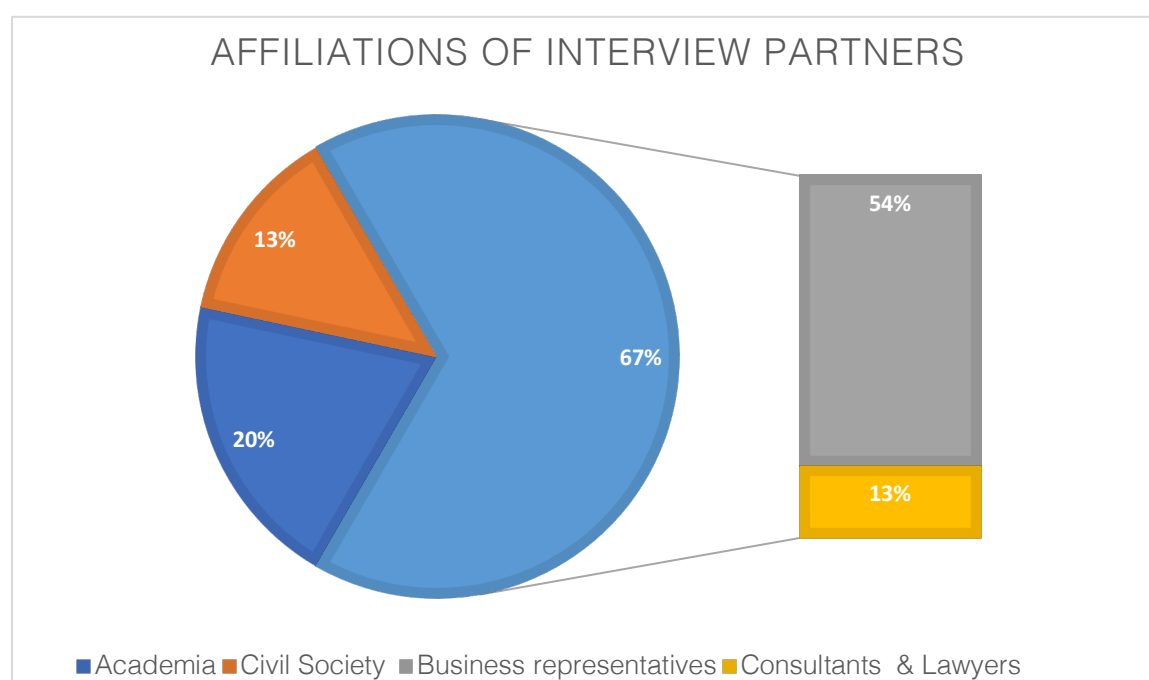


Table 3: Affiliations of interview partners (own illustration)

The vast majority of interviews were audio-recorded and subsequently transcribed (about 27 interviews of the 30 in total). Some interview situations would not allow for recording (the discussion took place in an unsuitably noisy location such as a busy restaurant or café), or otherwise due to confidentiality concerns of the interview partner. Interviews were made in person or over videoconferencing. If a recording was made, the person explicitly gave consent to being recorded based on a consent form that ensured anonymity and also the possibility of withdrawing any information at any given point in time (at the point of writing, no-one has taken up this offer). On one occasion I had to sign a non-disclosure agreement. I reflected upon whether or not to audio-record my interviews. Audio recordings enable a full verbatim record whereas taking handwritten notes can lead to substantial data loss. However,

interviewing without recording, in particular for in-person interviews, turned out to be more candid in a few situations. Taking into account the limitations on recordings in a few instances, it was not seen as a major impediment to extract the necessary information for the research interest and by deciding against recording, it made the conversation possible in the first place (Tracy, 2010, p. 839). If a recording was not possible, I took extensive notes. Some interviews were made over lunch, in a café, in an office or meeting room or via video conferencing, which proved that the mixed approach of adapting to the interview situation was helpful.

ID	Industry	Role	Scope of Business Activity
1	Telecommunications	Director of Supply Chain Sustainability	European company with significant presence on the Asian continent
2	Consulting	Senior Consultant	Senior policy professional with strong working experience on human rights issues in ICT
3	Law firm	Staff Attorney	Civil rights law firm
4	CSO	Director	Sub-Saharan Africa civil society organization
5	CSO	General Council	Digital rights organization headquartered in the USA with strong network across the globe
6	Telecommunications	Deputy Chief CSR Officer	Among top 10 mobile operators, European company with significant presence in Africa
7	Telecommunications	Human Rights and Security team (3 persons)	European company
8	Telecommunications	Senior Adviser Digital Rights	European company with significant presence in Central Asia, South Asia and Europe
9	Telecommunications	Director Public Policy & Internet	European based company with significant presence in Latin America
10	Conglomerate	External Affairs Specialist	European-US based company with significant presence in South America, Africa and Asia
11	Academia	Professor	City University Hong Kong
12	Telecommunications	Deputy Chief CSR Officer	European company
13	Consulting	Senior Policy Consultant	Senior policy professional with strong working experience on human rights issues in ICT
14	Academia	Senior Research Associate	Citizen Lab
15	Academia	Senior Researcher Security Studies	Swiss Federal Institute of Technology (ETH)
16	Consulting	Senior Legal Consultant	Senior legal professional with longstanding experience on human rights issues in ICT
17	Industry association	Policy Director	Senior professional with significant working experience in tech policy
18	Telecommunications	Senior Adviser Digital Rights	European company with significant presence in Asia and Eastern Europe
19	Academia	Legal Researcher	University of California, Berkeley
20	Academia	Digital Rights Policy Expert	Harvard Berkman Klein Centre
21	Academia	Senior Researcher Technology and Policy	Massachusetts Institute of Technology (MIT)
22	Platform	Senior Counsel	Digital intermediary with services such as advertising, cloud computing/storage, search
23	Platform	Privacy Policy Counsel, Global Policy Lead for Human Rights (2 persons)	Platform offering services in communications, search and advertising
24	Telecommunications	Senior Human Rights Manager	European company with over 600 million customers
25	Infrastructure provider	Head of Human Rights	Internet infrastructure provider
26	Infrastructure provider	Corporate Responsibility Expert	Internet infrastructure provider
27	CSO	Director	Digital rights benchmarking organization
28	Telecommunications	Senior Human Rights Manager	European company among the top 10 mobile operators, presence across five continents
29	Academia	Professor	University of Southern California
30	Conglomerate	Group Corporate Responsibility	European company, with a significant market share in Europe and the US

Table 4: Anonymized overview of interview partners (own illustration)

2.2.2. Access to the field

Discussing cooperation or non-cooperation with government actors on data requests is a sensitive matter for most companies. Often, the corporate teams dealing with these requests need to have security clearance. Hence, there were significant challenges in finding corporate representatives willing to be interviewed, and it

required a significant level of trust building over the course of more than two years to reach a solid number of interview partners that can be deemed as sufficiently representative for the field.

In some cases, introductions from one company representative to another helped to ensure high levels of confidentiality with interview partners. In particular, corporate representatives of platforms were reluctant to be interviewed. In response, the sensemaking process for platforms is partly reconstructed by talking to experts working with platforms (lawyers, consultants); nevertheless, a set of major players in the field agreed to be interviewed after having established a working relationship based on trust. In addition to the sensitivity of the contents of the interviews, busy work schedules aggravated the problem of access.

With regard to geographical spread of the interviewees, the majority are located in OECD countries and predominantly in the western hemisphere. This reflects the imbalance of geographical dispersion of capital and decision-making power in the tech sector, but at the same time reflects the global market share of the information economy that these companies inhabit, perhaps with the exception of the Chinese market. To a certain extent, companies headquartered in non-democratic regimes might not be prohibited from talking transparently about their conduct regarding user data requests, or might have direct access to user data by default. Nevertheless, information from interviews also showed that direct access provisions for the government can exist in democracies as well (ETSI, 2006). Also, local regulation in non-democratic regimes always affects companies headquartered in democratic and rights-respecting regimes which have offices and operations in non-democratic regimes (host states) as well.

2.2.3. Considerations on expert and elite interviewing

To a certain extent, expert interviews resemble elite interviews in that the majority of the interview partners were part of senior management or director level. Literature on elite interviewing shows that interviewees tend not to “suffer fools gladly” if the interviewer fails to show good command of the material (Richards, 1996, p. 201). Given that it is a sensemaking research design, I aim at distancing my own opinion as much as possible when analysing the data. Even though I had previously worked in the field, I did not have extensive work relationships with any of the interview partners. I left my job to be perceived as a more neutral researcher and not a human rights policymaker. Interviewing the elite bears an additional unique set of challenges such as information asymmetry in favour of the interview partner, and power imbalances between the interviewee and interviewer due to the potential higher status of the interview partner (Bygnes, 2008). Also, elites tend to be convincing and eloquent speakers: Delaney (2007, p. 215) raises the point that there is a danger of the interview partner “seizing control” and in consequence dominating the interview. This relates closely to the danger of the interviewer being taken in by the interview partner by their charm and power of persuasion (Delaney, 2007, p. 217). There is a

persistent information asymmetry between the interview partner and interviewer that could affect the data quality, e.g. would the interview partner potentially mislead the interviewer? (Berry, 2002, p. 679). The methodological lens of sensemaking sets the focus on the organizational actors' perceptions: the sort of reality the interviewer is constructing serves as the central object. Hence, to a certain extent, it is not critical whether what is said is genuinely representative. Sensemaking is essentially about the organizational members' perceptions and how these perceptions then shape their actions, and in consequence the unfolding of events. Nevertheless, what is said could still prove misleading as regards to how interviewees really perceive an issue. To a certain extent, it helps to speak to people with similar roles in different companies and experts outside of the private sector, as their opinions on certain facts often starkly differ. The decision to provide information only on an aggregate level was motivated by the fact that it makes interview partners more likely to speak honestly about their challenges.

3. Data analysis

3.1. Coding of interviews

The interviews were coded with broad thematic coding to let themes emerge inductively from the material and to re-construct the sensemaking around the corporate process in dealing with government data disclosure requests (Gioia, Corley, & Hamilton, 2013; Miles & Huberman, 1994; Strauss, 1987). Data collection through expert interviews gives insight into the sensemaking process in an organization. This requires a certain degree of data reduction in the process of data analysis: "coding serves the purpose of marking the islands, archipelagos, and other land masses of meaningful data from the surrounding sea of raw, uncoded data" (Lindlof & Taylor, 2017, p. 319). The fieldwork was ended when data saturation and information sufficiency was reached, as evaluated along the following three dimensions (Snow, 1980): (1) Taken-for-grantedness, meaning that a high degree of competency within a cultural membership was reached. This means that the interviewer understands the interview partners' world so well that the interviewer was rarely surprised or baffled by what interview partners said or did. It relates to the ability to comprehend the sphere of discussion. (2) Adding to this, theoretical saturation was reached when the continued observation only led to what was already known and resulted in repetitive information/field notes/memos. (3) Heightened confidence, meaning that observations and findings are deemed as showing a somewhat true picture of the "empirical world under study and shed light on pre-existing or emergent questions and propositions" (Snow, 1980, p. 104).

After a first review of the interview material, it appeared that the general themes from the sensemaking literature would be somewhat applicable as clustering categories for the emerging codes, as they are to a certain extent universal for a range of organizational contexts. Yet at the same time, it was not clear ex-ante how dominant

the presence of certain subcomponents in the clustering categories would be. The three dimensions of organizational sensemaking as proposed by Weick et al. (2005) that will lead the coding deductively are: (1) Organizational factors and structures before the crisis (agency of actors, interdependent and differentiated the roles in the organization, system tightly or loosely coupled); (2) Shared understanding in the organization (holding of different pieces of information by individuals, collectively constructing a new meaning, diversity of goals); (3) Early actions taken in a crisis (early actions determining outcome, inaction/absence of action). When reviewing the data before coding, and upon reflecting on the data, it became evident that the three dimensions will be suitable for the data analysis, with the only caveat being that the early actions taken in a crisis were in certain interviews not crystal clear, and only discussed in rather oblique terms. To a certain extent the semi-structured nature of the interviews helped to lead the interview partner to information of interest, nevertheless the willingness to disclose details of strands of corporate action differed starkly between interviews. Adding to the abductive use of the three dimensions of sensemaking, the research design allows for inductively constructed categories as they emerge while analyzing the patterns in the data (Miles & Huberman, 1994, p. 17; Strauss, 1987).

3.2. Retracing the corporate response to data disclosure requests

Midway through data collection, after “early data analysis” (Miles & Huberman, 1994, p. 50), it became evident that for enhanced clarity it was necessary to display how the process inside a company is structured before the coding began, as a baseline for the sensemaking analysis. For that purpose, I drafted a general “process model” to serve as a structuring point for orientation as to what happens when a company receives a data request (Lindlof & Taylor, 2017, p. 311). This model was subsequently refined with corporate interview partners and served as a helpful tool to gain more insights on differences and commonalities, and served as a “speaking instrument” in conversations with interview partners (compare V.1.).

4. Constructing dimensions

The interview material was coded with broad thematic coding and triangulated with the insights from the document analysis. Overall the assessment of publicly available policy documents confirmed the claims made by Soghoian (Soghoian, 2011) and Rahman (Rahman, 2016) on the insufficiently informative nature of transparency reporting with regard to numbers. The RDR (RDR, 2019) criticism of vague wording in public policy documents was also confirmed for the following three key reasons: 1. Policy documents re-iterate caveats and/or legal limitations on describing their actions, making most statements non-informative as they exclude a lot of situations as “out of scope” through these caveats/limitations. 2. Policy documents cannot show the full assessment process and/or fail to elaborate on the situational context. 3. There is a strong inconsistency in communications about data disclosure requests in the sector. The assessment of publicly available documents confirmed the view that the

data quality and richness does not suffice for an extensive document analysis that could shed light on actual managerial practice in dealing with unusual requests in conflicting jurisdictional settings, as claimed by various scholars and civil society experts previously (Parsons, 2019; Rahman, 2016; RDR, 2019; Soghoian, 2011). Nevertheless, some pieces of interesting information could be retrieved and will be assisting the construction of dimensions in combination with the insights gathered from the expert interviews.

The data analysis had to rely heavily on information extracted from expert interviews, as shall be described. Codes are “tags or labels for assigning units of meaning to the descriptive or inferential information compiled during a study” with an emphasis not on the words themselves, but their meaning (Miles & Huberman, 1994, p. 56). The codes are used to retrieve the information from the interviews and organize it. The coding was facilitated with the program “Atlas.ti 8”. The entire interview material was coded twice. In the first round was “informant-centric coding” (Gioia et al., 2013), closely related to the empirical interview material. For the second round, I increased the level of abstraction to group the participant-centric codes into “aggregate dimensions”. These aggregate dimensions are broader in scope and ensure an internally consistent way for clustering content through similar codes (Gioia et al., 2013).

After the initial coding, 108 codes emerged that were then iteratively subsumed into clustering codes and subcomponents, from a further reduced basis of 98 codes. Comparing the interviewees’ statements among each other, and juxtaposing them additionally with policy documents, various and often rival perspectives about the empirical phenomenon exist. An iterative manoeuvring through the data can capture those heterogeneous perceptions. Strauss (1987) suggests such contrasting perceptions among groups actually help to sharpen the knowledge process by understanding what is different about them.

I came up with a system to categorize the codes in order to make it more straightforward to find the relevant segments for the sensemaking analysis. These categories consisted of the three classical sensemaking categories as proposed by Weick et al. (2005) (Organizational factors and structures before the crisis; shared understanding in the organization; early actions taken in a crisis), as sketched before. On the other hand, in reference to the specific research interest and emerging themes in the interviews, five additional categories were constructed. These are: external environment, government relationship, process/routine for unusual requests, headquarter-subsidiary relationship, and human rights mindset.



Figure 4: Abductive approach to sensemaking themes (own illustration)

For increased traceability of the findings, the data structure of the sensemaking categories is displayed in Figure 5 and Figure 6, using the approach by Gioia et al. (2013), and depicts the first and second order concept, and how they lead into an aggregate dimension. To ensure a vivid account of the participants' observations through data thickness, the findings section relies on narrative quotes and short excerpts from the interview material.

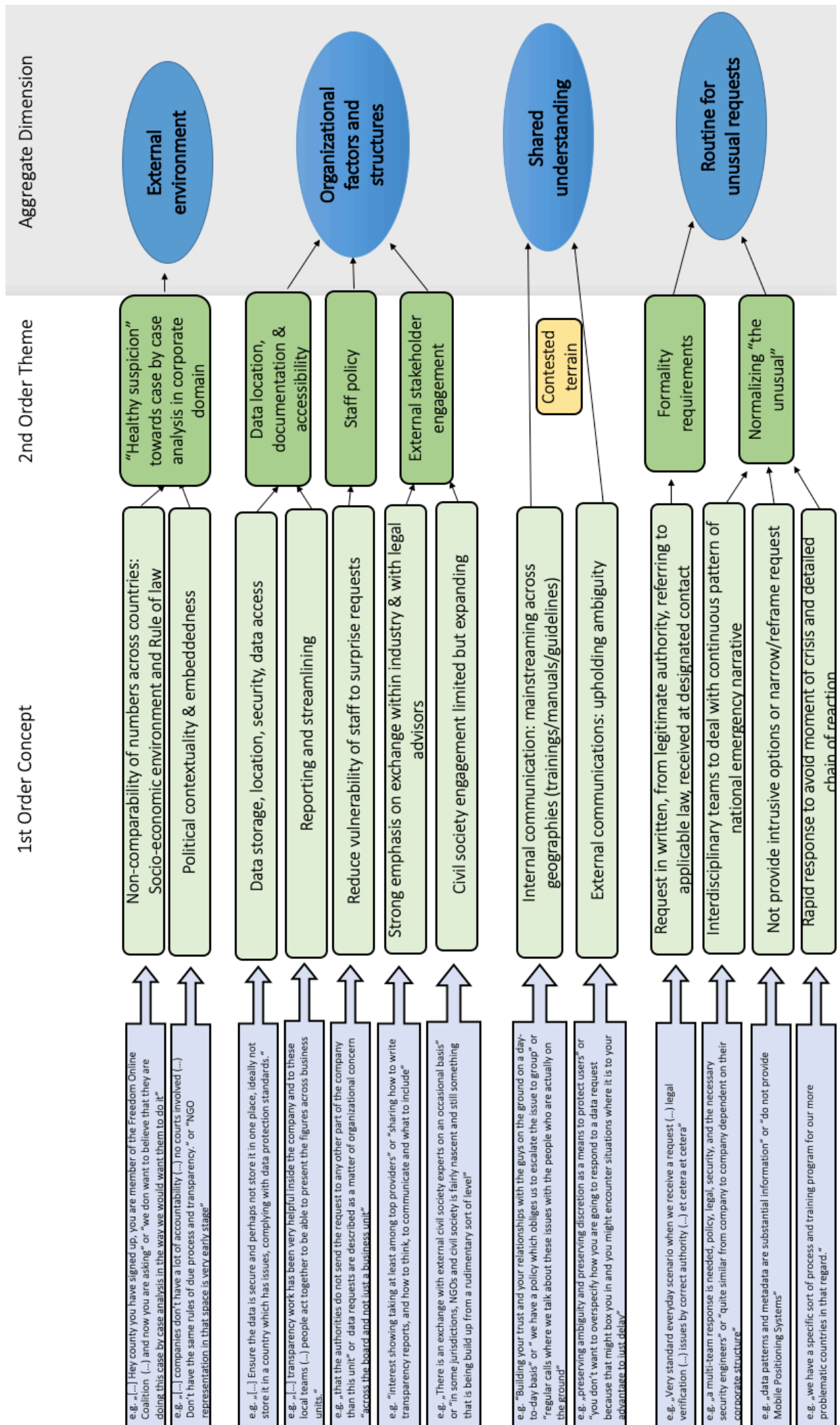


Figure 5 Sensemaking dimensions displayed using the Gioia-Scheme, part 1 (own illustration)

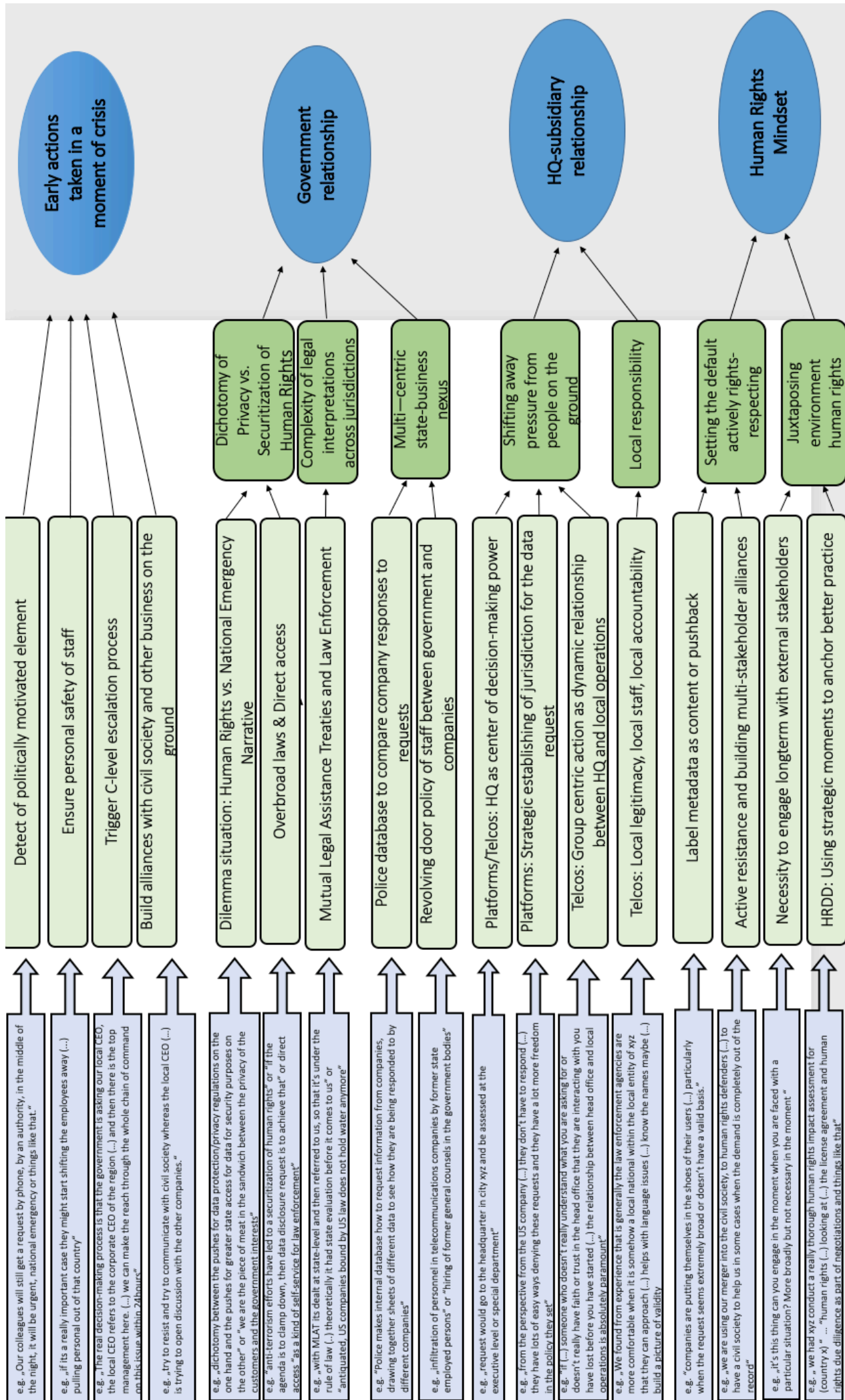


Figure 6 Sensemaking dimensions displayed using the Gioia-Scheme, part 2 (own illustration)

V. Findings

1. Retracing the sensemaking process in companies

Generally, the government can request data from a company in various forms. Interviewees also reported on requests received over the phone. Nevertheless, the majority of companies appear to assess the legitimacy of an incoming data request by four factors: it needs to be in writing, be issued by a recognised authority, refer to applicable law and be received at the contact in the company that was designated to authorities. This also clearly emerged in a range of publicly available policy documents. For example, Microsoft (GNI, 2020a, p. 60; Microsoft, 2020) points out the following information:

For government demands to restrict content, Microsoft requires a lawfully authorized legal order in writing (unless the applicable law allows oral orders) that is legally binding on Microsoft and complies with the rule of law. Microsoft attempts to comply with orders in a way that minimizes the impact on freedom of expression and provides information to users regarding generally applicable laws or legal demands requiring restrictions on content, and on Microsoft policies for responding to such demands. The CELA law enforcement and national security team, and an analogous team at LinkedIn, is responsible for government requests for user data. Under the policy for handling such requests, Microsoft does not provide governments with direct and unfettered access to customer' data. Microsoft only pulls and then provides the specific data mandated by the relevant legal demand. Requests are reviewed to ensure they are valid, to reject those that are not, and to ensure only the data specified is provided.

When these formal requirements are met, the company assesses the scope of the requests. This can include checking whether the scope appears appropriate for the indicated purpose, what might be the potential adverse impacts to persons implicated in the request, and review of the past record of the requesting authority. This assessment then determines whether the data is handed over as requested, whether the company delays the requests or otherwise asks the government to edit the request (e.g. to narrow the scope from an interpretative or technical side), or whether the company rejects the request outright. The transparency that Telia Company (2020) provides by publicly disclosing the assessment form is outstanding. The information in the assessment sheet appears to correspond with what other companies are describing in broader and vaguer terms, but provides much more detail. The form singles out five assessments the local company has to make: legal assessment (is the request formally valid, binding, possible to appeal); seriousness of impact on freedom of expression or surveillance privacy; is the request exact, is there any room for narrower interpretation; business impact of a) rejection and b) execution; and the risk to safety & liberty of company personnel.

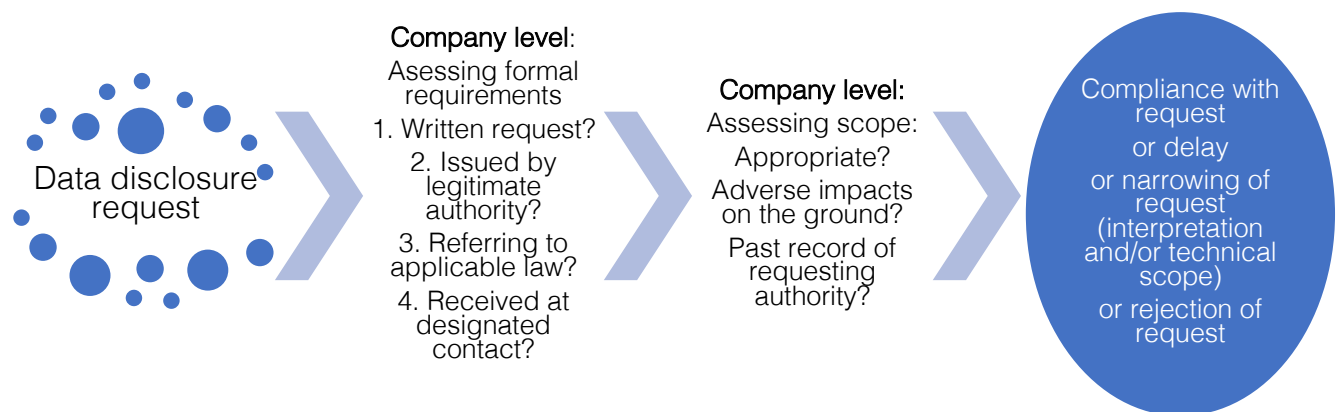


Figure 7: General process model of responding to a request (own illustration)

In sum, aggregating the publicly available information across the documents of a range of companies, if a request is in writing, refers to applicable law, and is made by an appropriate authority to the designated contact within the company, it is most likely deemed as a standard request, unless the scope is too broad and/or the political situation indicates a context where additional assessment is deemed necessary. At the same time, most interviewees had been exposed to unusual requests in highly politicized contexts, and were partly unforeseen. Instances have been recalled where the government called and wanted data within hours.

In the process of interviewing and analyzing the interviews it clearly emerged that the situation of telecommunications companies – which for the most case also act as Internet Service providers – and platforms differs substantially. Hence, the general process model consequently serves as the basis of two extended and distinct models: one model for telecommunication companies, and one for internet companies/platforms. The insights from the interviews showed such strong differences that it made two distinct models necessary, in particular due to the role of (1) local staff and infrastructure and (2) data location.

The basis for a telecommunications company to operate as a provider of telecommunication and internet services is a license agreement with the local government, in conjunction with standardization frameworks such as those provided by the European Telecommunications Standards Institute that ensure inter-operability across jurisdictions (ETSI, 2006). After checking the formal requirements, the assessment stage evolves around ensuring the integrity of the local staff and infrastructure on the ground against the backdrop of the company's human rights

commitments, but there might be tensions with the obligations under the license agreements with the local government.

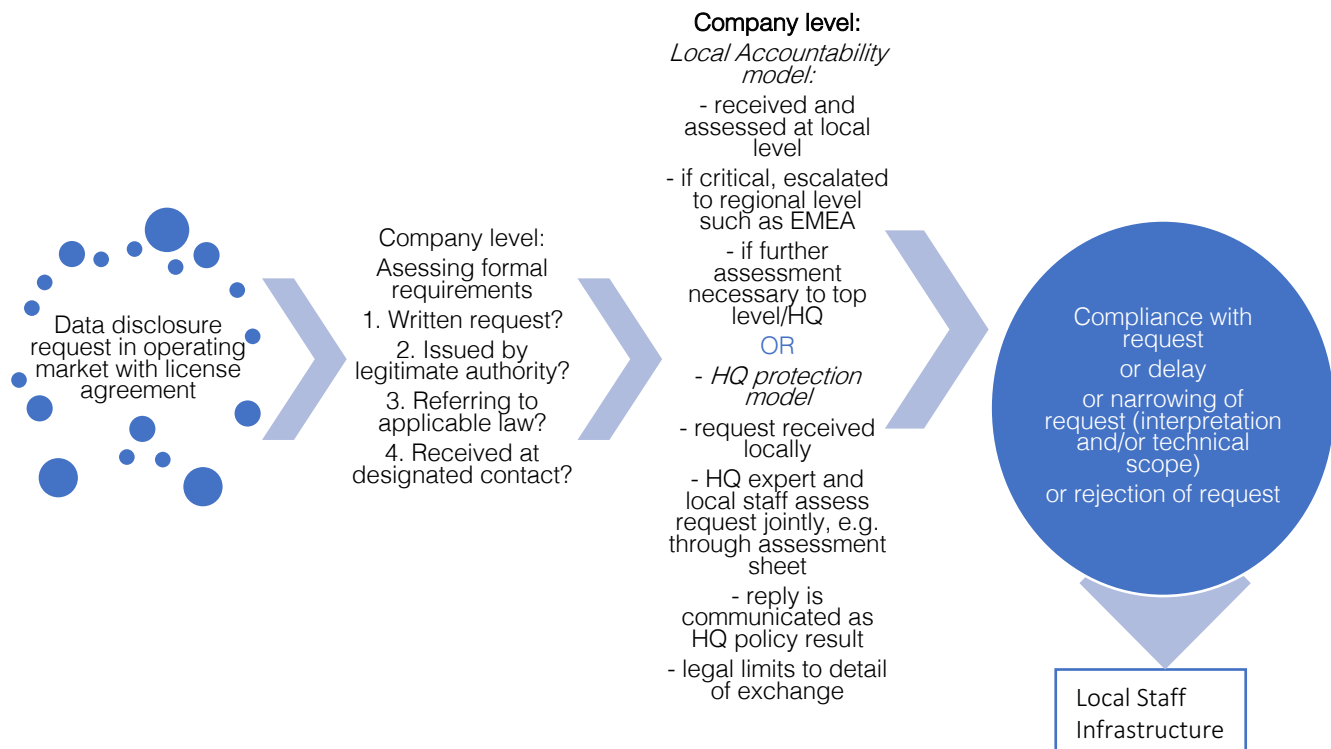


Figure 8 :Process model telecommunications company (own illustration)

With regard to (1) local staff and infrastructure, in order to offer their services, telecommunication companies tend to have staff and extensive equipment on the ground. A complication arises if a telecommunications company operates in-country using third-party services and therefore has no infrastructure themselves. Any government data requests would likely go to the third-party supplier for action. Also, (2) data location is mostly local as the core business is to provide communications and data processing/storage in the local market. Two models of assessment emerged: a first model was described as one which rests on local accountability, where the local staff assesses the request and only escalates it to the headquarter or group level if it is deemed very critical e.g. to a Europe and Middle East Affairs meeting. On the other hand, a second model was described which ensures a close communication loop between local level and headquarter/group level. Here, the request comes in at the local level, and the local staff assess the request with an assessment sheet or similar management tool that is jointly evaluated with the expert staff located at the headquarter/group level. These are the two trends in types of response models that interviewees described for the telecommunications sector.

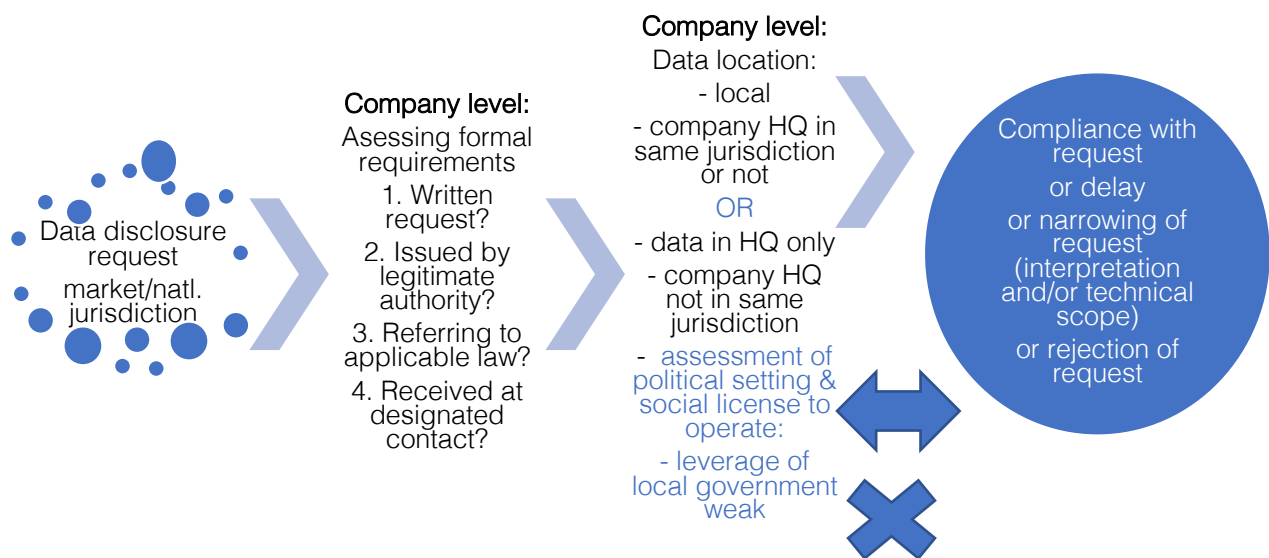


Figure 9: Platform company process model (own illustration)

Juxtaposed with the initial position of the telecommunications company, a platform operates in a consumer market of a certain national jurisdiction and is in a less formalized relationship with the government compared to the telecommunications company. Similarly, as with the telecommunication companies, platforms would verify the formal requirements of an incoming data disclosure request from a government body. Yet, with regard to 1) local staff and infrastructure, platforms often do not have a large number of staff in situ as their services are mainly provided online. Hence, the possible threat to local staff is a less important factor for platforms than for telecommunications companies. Even where the staff of the platform may be deployed locally, it is not necessarily the staff that could (technically) access the data, which might, for example, be stored in a different jurisdiction. Another key difference to the situation of the telecommunications companies lies with the (2) data location. In contrast to telecommunications companies, platforms may store data in data centres in other countries, and not necessarily within the same jurisdictions as the one where the request might come in.

As Figure 6 shows, if the requested data is stored outside of the jurisdiction in which the request comes in and the headquarter of the company is also located outside of that very jurisdiction, the leverage of the local government in requesting data is weak (see MLAT chapter III. 4.1.).

At the same time, the issue of the storage location of data determining what a jurisdiction can access was portrayed as rather contentious, and an unsettled matter. Given that data is often mirrored in the cloud and stored in multiple locations, even

knowing where data is stored is not always possible. Even among platforms, companies have taken different positions on whether it is the location of data, or where a company is incorporated, that determines jurisdiction.

These models still leave a lot of room for interpretation at the stage of the assessment of the scope of a data request. The coding of the interviews dives deeper into the perceived points of leverage and points of consideration, forming the basis of the sensemaking. The sensemaking dimensions will shed light on the underlying dynamics when companies react and assess the scope of a data request from a government body.

2. Sensemaking dimensions

To introduce the sensemaking dimensions, allow me to use a metaphor that one interview partner used – assessing a data request is like looking at a search warrant for a house: how many rooms do you allow the government to look at, and what sort of items will they search for?

2.1 External environment

What the process models have clearly demonstrated is that when determining the scope of a data request, there is potentially room for interpretation on the company side depending on how specifically the request is formulated, and whether it appears appropriate for the purpose indicated by the government. In return, experts working in the field have highlighted a "healthy suspicion of companies" is necessary. In particular in jurisdictions where platforms do business without local data storage and a relatively weak government position, "companies don't have a lot of accountability" (#3) as there are "no courts involved, they are not held to courts the same way that the government is and they don't have the same rules of due process and transparency that the governments do. So, there is a very healthy suspicion of companies". Publicly, a company might advocate for very progressive human rights commitments, while internally the assessment of data disclosure requests might follow a different path. Nevertheless, governments also exert a heterogeneous agenda that can cause competing institutional logics in a company. One interviewee stressed that the same government that signed up for key human rights instruments might counteract these commitments:

Hey country, you have signed up, you are member of the Freedom Online Coalition. You've said this and now you are asking. (#2)

It was repeatedly stressed throughout all interviews that international human rights law is not very useful in framing judgements as to the validity of unusual data disclosure requests, as few of the arguments will prove clear-cut with regard to potential impact (e.g. weighing privacy claims against the collective bodily integrity of a group of individuals when faced with a terrorist threat or an emergency situation) and, in particular, when the environment is such that there is little to no constructive

dialogue with the requesting authority. This is important to bear in mind for advocacy purposes. As one interviewee described:

There is an inherent tension (...) when we are demanding transparency from companies but also recognizing that (...) it is good for human rights that they are evaluating on a case-by-case basis. We just want to know – we do want to believe that they are doing this case-by-case analysis in the way we would want them to do it. (#3)

Interviewees saw pressure from civil society organizations as a considerable factor. Nevertheless in comparison to other digital rights issues, data disclosure requests were seen as one that do not (#5) “trigger a huge amount of fish” although they “think they should”, confirming the fact that “some metadata is as sensitive as, if not more, than content data”. For that reason, some companies have decided to work jointly with civil society organizations in a difficult external environment. For example, one telecommunications representative stated that (#12) “Human Rights Watch told me we have people on the site, would you like us to intervene” and that “Access Now will put it up on their blog”. This includes strategic work with the press, with one interviewee (#12) describing that a contact connected them to The Guardian: “so, I had an interview with not my name and the company this time to explain the behaviour of the government basically”. Yet, working with civil society organizations requires that these organizations have sufficient capacities in place on the ground. One interviewee stressed that (#10) “civil society is fairly nascent and still something that is being built up from a rudimentary sort of level” in some of the markets that the company operates in:

Given the real dangers that exist in being an NGO or a vocal activist in these countries (...) in particular as “a lot of these countries are also quite behind (...) in terms of the development of their ICT ecosystem and that’s kind of where we come in and we prioritize the connectivity and that digital infrastructure, but for the moment NGO representation in that space is in a very early stage. (#10)

Interviewees in that regard also repeatedly stressed the issues they are encountering when engaging on a data request or wanting to document them in fragile political contexts, in the global North, as well as the global South: “We are in 30 geographies, so we have an Excel sheet of 30 countries. There are a few countries in which we cannot talk, we cannot even record the numbers, so this is one thing” (#6). Adding to this, one “metadata request might stand for a completely different volume and granularity of data potentially than from another country” (#10). Even within the same external environment, a “request might actually be for one thousand different sets of metadata. It depends if we count a request as one written order and that may have two metadata versus one thousand” (#10). Interviewees agreed that the diversity in the sorts of requests lends itself to the type of disclosure granularity that actually adds value to the conversation:

At the end of the day, from my perspective, none of the telecommunications transparency reports really tell the full picture, the true story. The only one that

holds the overall picture (...) is the government. That are the ones that can really tell who is requesting what from all companies (...) I mean it obviously helps when companies are providing transparency reports because it tells something, but the overall picture maybe only sits with the government. They are the only ones that have the sort of full umbrella view of the requests. (#10)

The external environment conveys the embeddedness of the data request in the company's ecosystem. Yet ultimately the actual corporate options at hand will also affect how a company makes sense of data disclosure requests. For example, *prima facie* it might seem that a platform acting in a market with a relatively complex government might want to stay out of local politics as much as possible (see figure 6). Yet the external environment does not convey the whole picture. As much as the external environment might appear as a sort of "corset" for corporate behaviour, the actual corporate set-up as a starting point for the sensemaking can still substantially determine the trajectory of a data disclosure request. The following dimension therefore sheds light on the organizational factors and structures that a company has in place when a data request comes in.

2.2. Organizational factors and structures

The sensemaking along the internal governance structures as portrayed by the interviewees is in the spotlight for this dimension. For more clarity, this dimension is divided up into three sub-categories which are: a) data location, documentation and accessibility b) staff policy and c) external stakeholder engagement strategy. Across the three sub-categories, it has been stressed by an interviewee (#29) that the overall maturity of the organization matters, and how key personalities shape the organizational context of the business. The interviewee pointed to the historic example when Google was still run by its founders in 2006, while Microsoft, by contrast, was at another stage of maturity due to its older organizational existence and partly took another stance in the legal, political and social-public realm (#29). There were some instances where interviewees noted that it has been "down to the individual human, life experience, standing inside the company, relationships and trust in company" to convince people and shape "perceptions inside the company", a factor due to seniority in the organizations in combination with lessons learnt (#29).

a) Data location, documentation and accessibility

As stressed previously, data location plays a central role for the response process to disclosure requests by the government. Consequently, many interviewees highlighted how data location forms part of the organizational structures of dealing with data disclosure requests, and that it can be used strategically to avoid harm to rights holders and staff: "Ensure the data is secure and perhaps not store it in one place, ideally not stored in a country with issues, complying with data protection standards" (#5). Essentially, "where is the data" (#2) establishes where the government has the jurisdiction to ask for the data. Apparently, there have been relevant cases in the past of this, such as with Yahoo's Vietnamese subsidiary locating its data in Singapore, rather than Vietnam (Maclay, 2010, p. 87). Again, the issue of data location was

consistently seen as a matter for debate, due to evolving practices of mirroring data in the cloud and storing it in multiple locations.

On the documentation side, there is certainly an increased awareness among interviewees around putting in place processes that make dealing with a data disclosure request “trustful”, “to find a trace and a memory of every single demand” (#6). Again, in combination with the issues around confidentiality laws in tension with transparency reporting mentioned earlier, interviewees mentioned that there are structures or processes put in place to allow for enhanced documentation of disclosure requests, but the notification of users was rarely an option. Excerpts from policy documents show why this might be the case in transnational setting. For example, Google states:

Where data is disclosed to a government agency pursuant to legal process, Google will notify the user whose data was disclosed, unless it is specifically and clearly restricted by law from doing so. For requests from governments outside the US, this is generally limited to civil/administrative requests, due to secrecy laws. (GNI, 2020a, p. 58; Google, 2020)

Also, Facebook describes in its Law Enforcement Guidelines (Facebook, 2020), that Facebook’s policy is to:

Notify people who use Facebook’s service of requests for their information prior to disclosure, unless Facebook is prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies or when notice would be counterproductive. Facebook will also provide delayed notice upon expiration of a specific non-disclosure period in a court order and where they have a good-faith belief that exceptional circumstances no longer exist, and the company is not otherwise prohibited by law from doing so. (Facebook, 2020; GNI, 2020a, p. 52)

Nevertheless, civil society in particular highlighted the importance of “having a policy that will notify users if it is legally possible, as soon as possible, that’s a good policy and enables the users to defend their rights and then (...) regularly reporting” (#5). Nevertheless, even “mature” companies stressed that improving reporting and setting good standards has proven to be a journey (#12). The majority of interviewees stressed that data access and handling is only executed by a very small set of people, although they also placed a caveat here and highlighted that this is a characteristic of “mature” company conduct. Smaller companies or the ones less experienced with such requests might handle them differently.

One of the ways that mature companies handle this is by strictly limiting who has access to user data, if it’s just by credentials or that they can’t access it (...) it’s a strategy that is relevant for data requests, to ensure that it has to go through the process that they have set up because no one else has the means to access the data that has been requested. (#3)

It was repeatedly iterated that the "amount of people having access is very narrow, very limited, with years of background checks" (#24) and no other person than those that are officially responsible would be able to do this, in a heavily guarded setting. For example, there are specific operator terminals with which to correspond with the law enforcement agencies.

Certainly, the reporting of data disclosure requests has not been implemented in isolation from other organizational processes, but rather interviewees emphasized how auditing has helped to streamline efforts on the human rights aspect of data disclosure requests across the company:

Transparency work has been very helpful inside the company and to these local teams too, as I said, people act together to be able to present the figures, which we then publish. And also, to be able to be able to present verifying documentation in this case to (...) our auditor, when they come up and say how did you derive to these figures and these figures. (...) So, when we at group level contacted our local companies saying "we want to collect and publish statistics" for our transparency report, the statistics are also then audited by our auditor as these figures are part of our yearly sustainability reports. And because of that, our local companies needed to get direct orders. We have also done some work on streamlining how our different local companies count, and how they count, and present the statistics. That way we can only come that far because then of course the local way of working depends on the figure of the information and the authorities might have different ways of working. So, it will never be fully streamlined (...) between the different local companies. (#8)

To generate the necessary managerial buy-in to adopt measures such as reporting and auditing demands for user metadata by the governments, in the following section I will illuminate aspects of staff policy that were raised by interviewees in the sensemaking about data disclosure requests.

b) Staff policy & formal requirements

The telecommunications companies in particular stressed that the (local) CEO is structurally involved in the decision-making process on unusual requests, whereas for platforms it appears to rest more with the expert teams assessing the request. A company pointed out that the local CEO and group/headquarters CEO will be involved if an unusual request has to be escalated.

If that can decide and find it an issue we would escalate even further up, kind of C-suite level. You know, and potentially the CEO, there is always kind of that level. And the thing that is unique about the process and through the whole process, the CEO at local level will also be involved in the process. So, they are (...) immediately notified when there is (...) an unusual or challenging request. So, the CEO at local level and (...) us at group level, are informed and then depending on the seriousness of it and the complexity of it, it's escalated further up the chain. (#1)

This quote speaks very much to the point stressed in the telecommunications process model as to the assessment of a request by an interlinking of the local subsidiary and the group expert team.

As mentioned earlier, with regard to the formality requirements, the majority of interviewees agreed that their companies let authorities be informed of a designated contact inside the company to approach for a request. This is to limit the vulnerability among staff to surprise requests and to ensure only dedicatedly trained staff are contacted so "that the authorities do not send the request to any other part of the company than this unit" (#18).

With regard to the staff responsible for assessing the scope of the request, most of the mature companies had moved to a multi-disciplinary assessment team for unusual requests, although the legal departments in fact had quite a dominant representation across interviewees, along with security staff. Often, the expert group included a mix of "privacy, security, and legal and sustainability, public and regulatory affairs and communications" (#1). Some companies dedicatedly hired former government officials (#23, #14), such as former attorneys that could understand the mindset of the government better and were therefore capable of limiting a request.

The majority of interviewees reiterated that where a company complies with a request, the personnel who access and handle the data had gone through extensive security screening. A smaller set of dedicated company representatives intended to roll out data disclosure requests as a matter of organizational concern as a "more systemic across the board and not just a business unit cause that has really to do with where the focus has been, but also looking more broadly at all other business activities" (#1) (to be further explored in the next dimension on shared understanding). Part of this move could entail working with stakeholders outside of the company. The extent to which this was mentioned as part of the organizational structures in the sensemaking around data disclosure requests will be explored in the next section.

c) External stakeholder engagement strategy

Interestingly, law firms were perceived by several interview partners as helpful intermediate points of exchange and as assisting in constructing a level playing field of company conduct by advising clients in a relatively consistent manner. Yet this was also portrayed not as a given fact in a company's sensemaking of government disclosure requests, but rather as being subject to the political will of the client company. In particular, general counsels were said to have a vivid networking relationship in the San Francisco Bay Area, so in a sense there appears to be a momentum ongoing of joining forces to find conducive forms of conduct on data disclosure requests. With regard to exchange within the industry, the GNI and industry associations were seen as a point for joint learning. Strategic, long-term engagement with civil society overall appeared complicated, due to confidentiality agreements or laws inhibiting communicating about government data requests. It was common, partly superficial and not structured, yet some interview partners emphasized how

helpful working with civil society had been in complicated cases, also through "intermediaries" like Access Now.

Thus, on the one hand the senior management/executive management networking between general counsels among the leading platforms and telecommunications companies in the San Francisco Bay Area was highlighted "organizationally (...) at least among those top providers" (#5). While on the operational level, many company representatives agreed that it helped them to work together behind closed doors or with selected circles from academia and civil society, "sharing on how to write the transparency reports and how to think, to communicate and what to include and whatever. And (...) how to do public advocacy around that issue – so very helpful" (#18). Only one interview partner from a telecommunications company mentioned working with a company-level independent stakeholder panel on data disclosure requests that also involved an exchange with independent experts along with government representatives or organizations closely associated with the government (#9). To what extent human rights due diligence involved strategic long-term external stakeholder engagement (as required by the UNGPs) concerning data disclosure requests, remained quite unclear, but has been mentioned by two interview partners in the context of new market entries (#6, #1).

To sum up, external stakeholder engagement as part of organizational structures and factors that shape the sensemaking around data disclosure requests showed a mixed picture with regard to civil society engagement, and appeared to involve rather regular engagement within the industry (peer-to-peer) or with legal advisors – certainly partly due to the highly political nature of the subject matter. There is a distinction between what companies do on stakeholder engagement with regard to policy development and how they involve external stakeholders in response to specific government demands. On the former, companies might have substantial investment in this activity and develop relationships with civil society and others. However, when it comes to data disclosure requests, there are significant legal barriers (attorney-client privilege or acts like the Stored Communications Act in the US) to being able to confer with external stakeholders as regards a specific request. Nevertheless, this does not necessarily imply that company representatives had a lack of awareness or understanding of the seriousness of unusual data disclosure requests, and their potential impact on human rights. The next section explores what interviewees disclosed in view of the extent to which a shared understanding about data disclosure requests shaped the sensemaking process when responding to data requests.

2.3. Shared understanding

In distinction to the organizational factors and structures, the shared understanding in the organization relates to the construction of a collective meaning through discourse, but also to how individuals hold different pieces of information, and whether individuals aim at achieving similar goals or diverse ones. Communication through different mediums such as training or manuals might play a role here, but also

whom that particular communication targets as a recipient. Throughout the interviews it emerged that companies aim at constructing a collective meaning on the a) inside that they then use for strategic communication to b) the outside. One of the means to support a collective construction of meaning can be the strategic building of teams from different expert backgrounds. Overall, most interviewees related most to how the company communicates and raises awareness about data disclosure requests.

Systemic communication across business units about the impact of data requests appears at the heart of organizational sensemaking, yet companies deploy different strategies to achieve these means. Telecommunications companies with a big presence in various political contexts across the globe aim at mainstreaming across departments and business units:

Building the awareness on these issues and how they really impact not only on a local level but also on a regional level. Sort of, nothing is local anymore, everything is global, and it's showing them examples how, what can seem, sometimes what the local guys may think whenever they are isolated and (...) boxed in a process, is – okay this is a request from the government. It may even be someone who doesn't receive these requests often may get one. And this is sometimes how illicit request can be channelled. They target maybe someone who doesn't usually receive these types of request and the first response of some people can be "oh god this is from the regulator I better respond to this as best as possible" without understanding the implication that might involve. So, (...) the awareness-building across the company, not only at, not only with the usual suspects, the usual people that are involved in these processes, sort of top-down messaging to the whole company to the importance of these topics and what implications they can have for, you know, the users in question and the company in terms of the reputation fall-out that we have seen in the past (...). That sort of constant interaction and dialogue with the wider company at the local level can really have positive consequences about how these issues are managed internally. (#10)

Adding to this, an example from another company is that the local CEO (national business) identifies "local positions, whoever they are, whoever has that local position receives push emails with the policy and then with a short questionnaire which ensures that the person in question will have read the document to verify. So, you won't be able to answer the questionnaire if you haven't read the document" (#8). Having the local CEO in charge of ensuring the training efforts on disclosure requests can be an asset for acceptance within the organizations.

On the other hand, there exists also a more technocratic response (compare previous section on staff policy) where only a very limited, well trained and extensively security screened personnel would effectively be able to access the data. Hence, it is seen as a headquarter-expert-only issue that does not require broader awareness-raising across the company.

A mixed version of both types emerged from companies that find themselves on a journey towards finding the best ways to follow-up the evolution and to embed robust processes into the company:

“Most of the time, when I started two years ago, nothing was existing. Human rights issues were not an issue in my environment but now we are putting down strong processes and we are reporting the evolution and the roll-out of these processes within the company every year”. Everything about reporting is open and accessible, it is on our blog (...) and it is audited, it is assessed. (#12).

In order to assess the communicative aspect further, I break down the sensemaking dimension of organizational understanding into a) internal communication, and whether and how this then is mirrored in b) external communication.

a) Internal communication

Interestingly, some interviewees pointed out that they are in almost daily exchange with their business units on political affairs, and partly on the matter of data requests. The high frequency of communication with business units and/or subsidiaries was perceived as a major asset in dealing with government demands across business units/subsidiaries:

And that for me is the real key here: building your trust and your relationships with the guys on the ground on a day-to-day basis. Otherwise, you know, you can make the most illustrative sort of fancy nice looking report but if the data, the underlying data is provided by someone who doesn't really understand what you are asking for, or doesn't really have faith or trust in the head office that they are interacting with, you have lost before you have started. So (...) the relationship between head office and local operations is absolutely paramount to being able to a) deal with these situations in a rights-respecting but also safety-conscious manner and b) provide the kind of transparency and disclosure that external parties are seeking in regard to this area. That would be my big take-away from our perspective. (#10)

Internal exchange as a constant interaction and dialogue with the wider company down to the local level was seen as a desirable goal of organizational shared understanding and as a means to improve the management of data disclosure issues internally.

In contrast, certain companies had more of an organizational tradition of escalating data request issues towards the CEO – perhaps rather than broader awareness. But it wasn't clear-cut as to whether both logics could co-exist at the same time. "The real decision making process is that the government is asking our local CEO, the local CEO refers to the corporate CEO of the region – we have country CEO, region CEO and then there is a top management here" (#12). What became clear throughout half of the interviews is a sense of a shared understanding that is also characterized by competing institutional logics. So interview partners reported "having a lot of internal

discussions as well, in terms of license agreement and human rights due diligence as part of that" (#1) and reflected upon the fact that finding a joint response across departments as to how to balance the relationship with the government and uphold human rights due diligence requirements, and follow-up from impact assessments was a difficult undertaking. The ideal type of shared understanding was portrayed along the lines of:

A top-down approach, with a human rights policy or a digital rights policy that is passed by senior leadership and there's board level cognoscente and charges seeing it through who can oversee this response process and the interaction with law enforcement and give feedback within that company from these intake-level up to the higher level is important. (#5)

With regard to precise steps adopted within the company, manuals and guidelines were a commonly introduced feature, but the level of detail included and dissemination strategy differed. A former employee of a platform stressed that red flags, trigger terms and a decision matrix would be beneficial, and others pointed to the necessity that manuals go into quite some detail and provide very practical, hands-on guidance on how business units should be implementing policies. Again, in the telecommunications sector I witnessed the friction between ensuring local accountability and group policy commitments at the same time. One telecommunications company representative described it thus:

But what they can do is to say, "we have a policy which obliges us to escalate the issue to group". That they can do and the policy in our procedures makes clear that decisions on such unconventional requests need to be approved on group level. So, I then coordinate (...) helping the local company to escalate to relevant people on group level to approve (...) how to deal with the request, including when and where possible for (...) measures to respect the rights of users. (#8)

Adding to this, there was a key difference between the flexibility of platforms in contrast to the formalized, relatively mature handling of data requests in the telecommunications sector.

For example, do telecommunications companies "communicate" with law enforcement agencies through so-called Law Enforcement Agency Terminals that ensure interoperability between government systems and the telecommunications network's data infrastructure? At the same time there is interdependency: in a sense a telecommunications company would not be able to access, for example, content from Facebook, and in reaction, a government might ask for a partial shutdown to be put into effect if an internet service provider like a telecommunications company failed to comply. If a platform does not comply, that whole service might be shut down by the telecommunications provider ordered by the local government. This interdependency was perceived by almost all telecommunications representatives that I interviewed. There was a joint understanding across companies that the government might fall back onto the telecommunications network operator if a

platform fails to comply and disclose user information about a user who shared content deemed as “unlawful” by the government. Then again, the shutdowns would raise more public outrage and impact the rights of a large user group. With criticism towards, in particular, Facebook, in some interviews it was stressed that you cannot manage a company by the mantra of “Mark says...” in reference to Facebook’s CEO Mark Zuckerberg. Experts pointed to platforms’ need to catch up on a more grounded, systematic process to deal with data requests to grasp contextual complexities across the globe.

Not surprisingly, beside manuals and guidelines, training was a means often adopted for improving the shared understanding across the company about the sensitivity of data disclosure requests. For example, this could entail:

Regular calls (...) where we talk about these issues with the people who are actually on the ground, so that they are aware of the process (...) from a safety angle as well. So that people know they have kind of support (...) we have a regular check-in with them, but more regular with the legal and regulatory call that we hold across the globe. (#7)

This points to the fact that organizational learning was seen as a key measure to anchor a shared understanding, partly overlapping with trainings but requiring a feedback loop and organizational processes that seek to enhance the capacity of the organization to deal with requests. So-called “post-mortem type of analysis” (#6) as part of the GNI assessment process were seen as a great way to learn as an organization. These post-mortem case analyses were described as follows:

We have to provide used cases. So those used cases could be as old as two years old and when we can release information, meaning when it is safe, for the company and for the people on the ground, to release information, then we describe the used case. The description is of course assessed, and this is not a public presentation but at least it is within the multi-stakeholder platform (...). This is really to share best practice and try to correct the legislation in the future of what is good to be done and what is not good to be done. (#6)

This points to an important feature that was mentioned across a range of interviews – how previous exposure leads to a different level of awareness in the company.

Looking at the well-documented case concerning Yahoo! and Shi Tao, some of the interviewees stressed that such a moment of crisis could help to shake up organizational responsibility, ask how the team is integrated, demand board oversight and adjust management structures accordingly. It was described how the Shi Tao case enabled key people in the Yahoo! management team to implement a Human Rights Impact Assessment for data requests even before these were common practice within the industry. Also, cases which resulted in harm of their own management team were sketched, such as:

Our CEO was asked to provide information on the matter and was ambushed in this scenario and was imprisoned around two months in a very, very dire situation (...) has not returned to the company since. We eventually got (...) out, but I think (...) had to take some time off to recover mentally and physically from the traumatic experience. So, we have these experiences and we are very, very conscious and aware of the very sensitive and political situation that exists in a number of our countries. (#10)

Interestingly, few of these progressive efforts sketched in the preceding paragraphs can be found described in the public domain. The next section is going to describe how internal communication does not necessarily mirror how companies communicate externally about data disclosure requests, and their shared understanding of managerial sensemaking in response to these requests.

b) External communication

In contrast with a lot of internal measures in the process of being rolled out that aim to anchor a shared understanding inside a company as to how to make sense of a data disclosure request, the phrasing about the process of dealing with data disclosure requests in external communications is rather opaque and vague. Interestingly, throughout the interviews the little information made available on requests that can be displayed in transparency reports was stressed and portrayed as a major limitation for external communication. This is also supported by the analysis of documents. The 2019 RDR edition ranked 24 companies based on 35 indicators, such as AT&T, Apple, Baidu, Facebook, Vodafone and Telefónica. One of the most contested issues in the tech space that RDR deals with are data disclosure requests (RDR, 2020a). With regard to government demands, the 2019 index summarizes as follows:

Transparency about demands that governments make of companies is also uneven and inadequate. Companies disclosed insufficient information about how they handle government demands for access to user data, and to restrict speech. As a result, in most countries, government censorship and surveillance powers are not subject to adequate oversight to prevent abuse or maintain public accountability. (Ranking Digital RDR, 2019)

Adding to this, an evident rise in government requests for user data from internet and telecommunication companies is visible in the corporate transparency reports, such as those from Google (Google, 2020) or Telefónica (Telefonica, 2020), or the RDR Index (RDR, 2019). In combination with this, companies consistently repeat a caveat on transparency: that the company will only report on user data requests if it is not prohibited by law from doing so and the actual description of the assessment process is close to absent. 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 (Microsoft, 2020).

Nevertheless, Microsoft supposedly 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. For example, Telefónica (GNI, 2020a, p. 77; Telefónica, 2020) publishes an annual Transparency Report related to requests from competent authorities regarding legal interceptions, access to metadata, blocking and filtering of contents as well as suspension for services. There is a range of countries for which Telefónica indicates that it could not disclose details of requests of communications data, demonstrating the limitations of public communications about such requests.

Yet publicly communicating in a vague manner around the processing of data disclosure requests is seen as a strategy to leave room for internal manoeuvres – and as a way to shield potential victims from harm caused by the impacts of data disclosure. In particular, legal experts appear to advise their clients that "you don't want to over-specify how you are going to respond to a data request because that might box you in and you might encounter situations where it is to your advantage to just delay" (#3). To elaborate on this important and somewhat surprising aspect of external communication about a shared understanding, the same interviewee stressed that preserving "ambiguity whether they would respond to requests from these countries" can be "a persuasive argument" (#3).

We like transparency and we do not necessarily believe that reasoning that companies give us about some of their policies and we try to be sceptical but in our estimation that we don't want to do harm to the users in those countries; that is the opposite of what we are trying to do here (...). So, I have basically heard about that strategy of preserving ambiguity and preserving discretion as a means to protect users. (#3)

Such lines of argumentation on ambiguity have also to be read with the notion in mind as to the external environment (see dimension 1) and a "healthy suspicion" towards the black box of company conduct.

In contrast however, opportunities for whistleblowing were very rarely mentioned. Whistleblowing structures to alert the company to potential wrongdoing appear not to be very common as regards data sharing with government. This, again, is most likely due to confidentiality and national emergency legislation. Only one interview partner mentioned this.

They are asking us to have a grievance mechanism process which is a whistleblowing – very active whistle-blowing and very open whistle-blowing – process. We had one for only ethics in the company but the fact that we have to, and this is always the same thing, that every time there is a law, it helps the company to build the processes. So, we are putting the whistleblowing, this open whistle-blowing process up, it is not up and running now but it will in a few months from now and so it's a big change for the company. And human rights and environmental issues will be able to be addressed through this whistle-

blowing process and it will be accessible anywhere, it will be an internet link for grievance procedures. (#12)

Even in this example it remained unclear how this grievance mechanism would work in practice with regard to data disclosure requests, as it was only at the implementation stage at the time of the interview.

To conclude, creating a shared understanding when responding to data disclosure requests appeared as a contested terrain in respect of these requests in organizational sensemaking. A core aspect stemming from the interview material was the conflicting institutional logics on how much awareness is necessary across “ordinary” staff, and whether it is sufficient to delegate the complex materiality of data disclosure requests to a small set of people with the expertise to assess the scope, and then hand it over to the experts who can assess the data, or whether a broader awareness would be beneficial to counteract oppressive government tactics. It appeared that there is as yet no industry consensus about the best way forward. At the same time, exposure to threats in the past has led to a re-thinking of managerial sensemaking. This certainly impacts if, and how, the companies have decided to construct a sort of routine process for unusual requests. What could constitute such a routine process will be described in the subsequent paragraphs.

2.4. Routine for unusual requests

Interviewees portrayed the managing of some unusual requests as a routine action that either made a standard scheme or a slightly adapted scheme for the context necessary. At the same time, there was also a distinct portrayal of unusual requests that constituted a moment of crisis for the company. The distinction between the two is caused by specific triggers, which will be explored in the following sensemaking section about unusual requests that were interpreted as a moment of crisis by the interviewees.

The set of formal requirements that were stressed by most of the interviewees as being necessary were: that the request be in a written format from a legitimate authority and referring to applicable law, and received by the contact inside the company designated to the authorities. One interviewee gave a summary snapshot of the requirements for a request deemed as standard.

A very standard everyday scenario when we receive a request from a judicial authority and we will conduct a legal verification of the order to make sure that it matches all judicial requirements or legal requirements and that it's issued by the correct authority, that it specifies the correct legal authority under which they can make the request et cetera et cetera and then we will proceed to search our databases in accordance with the request and provide a response to the requesting authority based on our results. (#10)

Company representatives defined unusual requests as the ones for which either the formal requirements were not quite met but the government exerted pressure, and/or

where the formal requirements were met but when the company assessed the scope of the requests, the decision-making process needed additional measures than for standard requests. In the discussion that follows I will explore the routine process for these sorts of unusual requests, whereas the subsequent sensemaking dimension will explore early actions taken when an unusual request has triggered a moment of crisis. Interviewees stressed that in many cases the GNI implementation guidelines in particular might be more detailed in terms of the specific commitments around how companies deal with demands, than the company's own public facing policies on these issues.

Firstly, in the routine process of dealing with unusual requests, interdisciplinary teams with human rights expertise were seen as a way of dealing with the full spectrum of the contextual factors that might influence how sensitive a request is deemed, and why exactly it is deemed unusual. Most of the time, an unusual request is assessed by an interdisciplinary team with human rights expertise as a "multi-team response is needed, policy and legal, security team and also the necessary security engineers to ensure there are other ways to secure the systems" (#5). Whereas the exact names of the involved business departments might differ, the actual staff and their professional background are:

Quite similar from company to company dependent on how exactly their corporate structure is named (...) the functions are essentially the same from company to company but they would just have slightly different names and slightly different structures in terms of grouping legal or separating certain functions from others but in general you have (...) legal definitely involved as a very key actor, compliance is there, too, and external affairs (...) a function that incorporates regulatory affairs, corporate responsibility, government relations and corporate communications. (#10)

Some companies work by setting up "law enforcement disclosure committees" or similar. As a trend distinguishing platforms and telecommunications companies here, telecommunications companies (#24) had a tendency to work more closely with teams such as "Group Corporate Security" or "Infrastructure Security" in multi-disciplinary settings, whereas platforms had a tendency to collaborate under the lead of legal experts (#23), for example weighing jurisdictional questions (see also staff policy under the organizational structures and sensemaking factors dimension). To avoid the complicity of their products in human rights violations, some companies that also sell equipment as part of their business (#26) mentioned that in certain fragile political contexts, by default they do not provide specific intrusive options in their technologies, such as Mobile Positioning Systems (MPS). If the responsible expert team were to assess a market as politically fragile, the MPS functionality would not be included in the technology sold to the respective government.

Companies mentioned that they have started bringing investors into this debated terrain and strategically aim at using investors' interests as a defensive argument by stating they would comply with the data request but (#18) "have to report about this incident to the Stock Exchange". Interviewees (#5) mentioned also that civil society

organizations in the investment and human rights field such as the Alliance for Human Rights have started working on the human rights impact of ICT products and their data footprint, along with responsible investment institutions such as the UN Principles for Responsible Investment. This would imply that a range of actors in the investment space could be moving into the ICT & human rights field in the coming years, demanding human rights policies. Ultimately, “investors want disclosure, right? They want transparency, it is the foundation for them” (#8). Hence the initial small number of telecommunications companies and platforms starting to engage with investors when faced with unusual requests by government actors that might be growing in volume.

Perhaps investor engagement might not be the case for each individual request, but might help to act on a general tendency that has been witnessed by interviewees throughout the field. In contrast with what the language suggests, data requests using a national emergency or national security narrative do not necessarily relate to very urgent security or emergencies matters. Rather, governments labeling requests as a matter of national security or emergency has become a prevalent pattern for most data requests by governments to the big tech players, whilst governments have also at the same time placed constraints on public communication about these requests in many jurisdictions. So even if companies would like to seek assistance or build alliances to cope with a profusion of unusual requests through “routine channels”, with the requests starting to constitute a pattern, “depending on national regulation, it might be tricky to discuss that with a group where it is deemed as concerning ‘national secrecy’” (#28). If even the company itself cannot assess the requests beyond the local level, this demonstrates that working with experts even outside the actual company will hardly be possible at all. A set of interviewees mentioned that a gateway for when the local team is not able to disclose information about an unusual request it might have received is the guidance provision put in place for finding another way to deal locally with the issue – perhaps by involving the executive level as soon as possible (see also the sensemaking dimension on shared understanding).

From a civil society side, the situation around national emergency or national security framing was made sense of as following:

We had some scenario in (country x) that was that kind of situation but unfortunately, we couldn’t confirm exactly. So we had to confirm the request from government was sort of shrouded in a bit of confusion so the request wasn’t... it didn’t specifically... the request for particular data or take down any specific name, you know user name or anything, but our suspicion was it was around some of the work done by activists. But it was difficult to confirm that. It was around national emergency and when national security and national emergency are issued there is sort of a brick wall. (#4)

Interestingly, only one interviewee saw this government agenda justified under the narrative of fighting crime and prevention of terrorism and pointed out that one has to differentiate between data protection/privacy in democracies “where users want the

government to know about certain data” for fighting crime and terrorism, where a bomb goes off, between non-democracies” (#2). Others agreed that the extent of data requests under this narrative of extraordinary measures, as required for national security or emergency, goes beyond what is acceptable and appropriate.

Nevertheless, the company representatives also demonstrated that the companies are very well aware in their sensemaking when replying to data requests from the government that under certain political circumstances or purposes, a very rapid response is necessary to avoid a moment of crisis. Many companies have put a range of measures in place to respond swiftly if they see signs of a situation potentially escalating, or if they clearly recognize that the political situation is indeed particularly fragile, as described in the following example.

So, there is quite a significant sort of weight on the Africa region and we have a specific sort of process and training program for our more problematic countries in that regard. So, they follow the same policy guidelines that I just mentioned but we also had to allow for the very sort of severe security situations that some of these countries can find themselves in. So [country x] for example is engaged in warfare with [intl. terrorist organization] and a number of other military operations in the region right now and for those reasons we expand quite a high number of extraordinary requests in that country. And again as you said from the outset, and I am comfortable that you understand the sensitivities involved, but I have to really re-emphasize the nature of this, the sense of nature of [country x] and the fact that no specific comments can be attributed to that country from this conversation as there are a lot of ongoing security operations that we are very conscious of not upsetting. (#10)

Other companies stress that in their sensemaking it is clear that structures have to be in place to provide guidance as, in "gunpoint experiences (...) there would not be time to give advice" (#24). Hence interviewees (#10, #24) reported they had put in place something like a law enforcement and major events guidance, requiring the interdisciplinary teams to analyze the request, taking into strong consideration the political events of the period and prior major events in the country, to decide whether to proceed to authorize the request or not.

At the same time, besides providing market-specific and detailed guidance that supports a sort of routine process to deal with unusual requests, some companies with a greater level of maturity aim to understand the government's intention to ensure a response that will satisfy the government, but also push it towards the side of the spectrum of possibilities that protect the users better. This was by no means a majority response, and should to a certain extent be considered as a relatively bold gesture depending on the government counterpart the company is facing. The same platform (#23) representative mentioned that the majority of data disclosure requests are about users' accounts. To elaborate, the practice of a platform dealing with a data request about information on a specific user account, or how to identify a user account, can relate to different purposes. If the platform can understand the exact purpose, it can tell the government to re-frame what it is really looking for and adapt the identification

measures accordingly e.g. narrow the request by time stamp x and/or location y. That very same platform displayed how the sensemaking of the company interprets overly broad or unspecific data requests as a very intrusive action that might convey an intimate picture of somebody's life.

Responding often to overly-broad requests would mean including information that has nothing to do with the actual issue for which data is requested. This is in agreement with another expert (#29) who stated that "data patterns and metadata" are substantial information. The same platform used a second tactic to protect its users from intrusive action – it labeled requests for metadata that met a certain threshold as "content" so that the burden for the government to access that data is higher, as "content" of communication is more protected and the requesting hence less easily justifiable from a rule of law perspective.

The notification of users was only mentioned by one interviewee and might potentially be connected with legal restrictions that do not allow for user notification under national emergency law. Nevertheless, despite the shrinking space for external stakeholder engagement about unusual requests, interviewees described their sensemaking around certain ways in which public advocacy about unusual requests is possible. A handful of companies described that they seek public advocacy measures if requests get complex e.g. through partnerships with civil society organizations. At the same time, companies stressed that this is a difficult task when civil society are not fully granted rights in some political contexts.

If the demand is OK, then we just obey the demand; then again we are trying to engage but many times it's violent. We are trying to engage with the governments. And it's very new in the last few years we are trying to engage with our competitors, trying to check what they will do. And if we have a set of telcos that are refusing the demand because it's not well presented or it's out of any context, then we try to move together to open dialogue with the government. This is one way. The other way that I am pursuing myself is to try to work with a supranational institution and here I am talking with the United Nations and I have been with many of the telecommunications companies within the Industry Dialogue and the GNI I have been very close to the Special Rapporteurs. I have been asked by the United Nations Human Rights Council to present a company case in front of the members where they were all in the room and it was very impressive and more recently I am engaging with the European Commission which is again both the Commission and the European Council, the Council of Europe. Very, very recently and we are signing (...) a kind of MOU with the Council of Europe in which we and many other companies will sit for regulation with the European Council to help them regulate the problems of privacy, discrimination, illegal content and all those things on the internet. And that could be one way also to reach governments via the regulation that the European Council is taking on this subject. (#6)

In summary, all the above measures can be part of the routine process of a company to make sense of an unusual request that is somewhat covered by routine processes. Then, those measures can lead to the conclusion that some requests are deemed as too broad and require a narrower interpretation, or, if not, a full pushback. One example of such a pushback – but also its (financial) fall-out – is described in the following interview passage by a telecommunications representative:

They can ask for – and that is the one we resisted, and I am very proud of it because we succeeded to resist – where they ask all the customer data. I mean there is a country in Africa that asked us, just to make sure we are paying the right amount of taxes, all the customer data, which is where you live, how many kids, what is your bank account and things like that. And so, on that one we refused and resisted, it was very heavy on us because we were taxed very heavily but at least they stepped back. So, the nature of data that can be asked is everything because technology can provide everything. (#12)

By understanding better what sort of unusual requests were deemed as a relatively “standard unusual request”, it became clearer which unusual requests really constitute a dilemma, for which even preventive measures in the routine process will not deliver an appropriate response. In the subsequent section, I will explore which unusual requests are deemed as major events and crisis moments inside a company.

2.5. Early actions taken in a moment of crisis

This dimension explores how interviewees made sense of how early actions determine the response to an unusual request that is interpreted as a moment of crisis. Some of the sensemaking practices when responding to an unusual request with a routine process might apply, but the process will either not have any impact or insufficiently address the dilemma situation in a crisis. For example, cases that do not comply with the formal requirements (in written form, legitimate authority, applicable law, designated contact) were described by a telecommunications representative as follows: “You know our colleagues will still get a request by phone, by an authority, in the middle of the night, it will be urgent, national emergency and things like that” (#1). Some interviewees referred to those cases as “major events” implying that (#10) there is a politically motivated element to the request, and/or the request is not aligned with international standards or norms of freedom of expression or privacy. At that point, some companies have put a policy guide for local operations in place that specifies the different scenarios by which a certain request is deemed a major event. This would then be the point at which the local operations will initiate an escalation process and report the situation to a senior set of individuals (#10) who are involved in these processes. This is particularly true for telecommunications companies, and in particular those that follow an assessment model for data requests that rests heavily on local accountability (compare telecommunications process model figure 2), rather

than exerting the joint assessment between headquarter and subsidiary at an earlier stage.

In particular for the telecommunications companies with staff and infrastructure on the ground, often the first priority when making sense of crisis situations was the threat to local staff and ensuring their personal safety. This was less the case for platforms, as they mostly steer data requests toward headquarters and are not bound to license agreements. Telecommunications companies in contrast described having an interdisciplinary expert team available 24 hours/7 days a week in different time zones around the globe (depending on the geographical spread of their operations) and/or a crisis response team ready to communicate to the government within 24 hours. The emergency sensemaking process was described as follows:

The real decision-making process is that the government is asking our local CEO. The local CEO refers to the corporate CEO of the region – we have a country CEO, a region CEO and then there is a top management here (...) in [European city]. And when the message comes to [European city], then I am in the loop. And I do my part which is try to resist and try to communicate with civil society whereas the local CEO with the help of the corporate chief is trying to open discussion with the other telecommunication companies first and with the government (...) It's usually very fast, it's an emergency situation – we can make the reach through the whole chain of command on this issue within 24hours. (#12)

If issues are re-occurring, staff are strategically relocated to another jurisdiction to avoid harm.

The really large companies, they get to a point where they have presence everywhere, but even then they may, and again I am not sure you would be able to get them to say this to you or publicly, if it's really an important case they might start shifting the employees away, kind of the way countries to when they run into diplomatic tensions and they're afraid about escalation to war, something like that, they might starting pulling personnel out of that country. I heard of internet companies doing that sort of thing as well. (#3)

Adding to this, there is also an interdependency between a company not disclosing information and the government in retaliation asking for (partial) network shutdowns: "what could happen is they are asked for specific data (...). And if they don't provide that, what can happen, is that (...) the government probably then comes to the operators and demands that they block those services" (#2).

In summary, it clearly emerged that a lot of weight rests with the government itself as the requesting body in such moments of crisis, how the government will react when the company cannot cooperate for a range of reasons, or whether the government is open to negotiating certain characteristics of the requests. To this purpose, the following section will explore how companies included their relationship to the government in their sensemaking.

2.6. Government relationship

The bare minimum the public knows about data requesting practices by government to private sector companies and the private sector response is documented in transparency reports and publicly available information on law enforcement assistance. Yet this is only the tip of the iceberg, as the relationship between government and private sector companies as regards data sharing practices is multi-centric, complex and highly dependent on contextuality. The limitations of the transparency reports in terms of representativeness of figures and limitations of reporting imposed have already been explored in the previous chapter.

Overall, on a broader policy level, what most companies were struggling to address in their sensemaking on government data requests is the crossroads they find their business at in respect of a security narrative and increasing data protection/privacy regulations. Interviewees perceived a "dichotomy between the pushes for data protection other one hand and the pushes for greater state access to data for security purposes on the other" (#5). Further, some interviewees were puzzled by the fact that on the one hand, a state is a signatory to various international human rights laws and on other the other hand "anti-terrorism efforts have led to a securitization of human rights" (#28). For most of the companies, there were no easy answers to this situation, as certain data requests appear justifiable in some contexts, yet they saw a lack of oversight mechanisms to hold the government to account.

Civil society experts working frequently with telecommunications companies and platforms stressed that businesses are also in the middle of the "fire" between activists and oppressive governments, to the extent that if the government interprets the situation as a loss of control, it might aim at silencing opposing voices, by both data requests and dataveillance and/or network shutdowns.

If the agenda is to clamp down, then a data disclosure request is to achieve that. And if the agenda is to clamp down, in the same way, the objective of a data disclosure request or shut down is basically to make sure there is no opportunity for either activists or people who work around these issues to have a free opportunity to work. (#4)

And exactly with this set-up, the ways in their power in which the government can be held to account also shrink, as the legislative branch of government has or loses independence: "I think when it gets to other countries, especially with telcos (...) it began in Sudan and other situations, you see the courts are providing more relief than analysis, no-one is stepping up" (#5). Again, it depends on the political environment in the country. Some telecommunications representatives also stressed that:

There is democratic oversight, there is an oversight body, kind of a court, there is a legislation etc. Whereas in far-away countries there might be less democratic oversight. There might be also less information about the law. (...) often in

countries where there is direct access, information received by the authorities to direct access might only be available to restricted authorities such as secret police and military. (#18)

This quote indicates an interesting development that company representatives pointed out continuously in our conversations: instead of countries having to request data through the corporate response process, they might require companies through legislative measures to give them direct access to their data, or specific parts of their data. For example, the Investigatory Powers Act in the UK risks resembling a kind of “self-service” for law enforcement. This then implies that “the company cannot count, (...) cannot make statistics and publish how many requests we get, so this type of direct access is critical from a freedom of expression or privacy point of view” (#7). In part, companies try to de-motivate the government from establishing direct access by arguing that the financial burden of upgrading the direct access system needs to be approved under the group procurement policy first. This was described as follows by a telecommunications representative:

It could be for example upgrading of the direct access system because there is a new generation of mobile service. Then many times also in some countries there is also an obligation by law on the operators to stand the costs for these upgrades of these systems. So, when there is a request for upgrading procurement needs to be involved, such procurement process cannot start until there is a group approval from the human rights team in the equation. So I will explain it in this way. Before we had a policy: if there was such a request, a request in such a market, then maybe someone called someone at group, someone at the local level called group or emailed group, and then maybe someone at group said okay, this is according to local law, then yes, then we comply. But with our policy and in accordance with the UN Guiding Principles on Business and Human Rights we are... we have a responsibility to respect freedom of expression. (#8)

How effective such a move will be to push back against direct access measures is not clear in the long term. Some interviewees pointed out that government might also increasingly be developing stand-alone technology by itself and that companies “might be out of the subject in few years from now meaning that the government should be completely independent, and they will have a stand-alone technology to do whatever they want. Which is a trend, it’s not happening everywhere but it’s happening in many countries” (#12). At the same time, the quality of the data in corporate hands is such that it will be very tempting to tap into from a government perspective for many years to come.

The hunger for data from government bodies was a major concern throughout all interviews and most interviewees highlighted that “governments are (...) happy to see that (...) they can be granted access to that data (...) on that collection piece” (#5). Telecommunications representatives perceived themselves as the “piece of meat in the sandwich” (#12) between the privacy of their customers and the government’s interests, which challenges them.

This is not sustainable. I mean we cannot be... we are a company with a backbone, with an ethics, we would like to do our job. I am responsible for behaving in terms of human rights issues in the company and the company gives me the power to progress but still, we cannot do the business the way we want, which is the way ethics and human rights issues tell us how to do because we are in between demands from customers which is also not also very easy to tackle because they want privacy but at the same time they give away anything to anyone, so this is the other side. (#12)

This dilemma came up repeatedly throughout the interview material. At the same time, in the sensemaking process in response to data requests, the government is not perceived as a homogenous, monolithic institution. Company representatives are well aware that branches or departments differ in their attitude towards the significance of privacy, yet ultimately who can access which data inside the government institutions remains in part unclear. The following quote describes this situation.

But it doesn't always mean that, either because one authority in a country would have access to that direct-access system but another authority that might need the information for another investigation might be not related to, it might be related to something else, a financial crime, it could be a different authority and they might not have access to that direct access system so they will request interception from us. So, there are a number of different factors that will play into the level or number of interception requests that we receive, that really blurs the lines and makes it difficult to say, oh yeah, that's a rising trend here because of X, Y and Z. There are just so many things going on in the background that we may have knowledge of or may not have knowledge of because of the sensitivities that are involved and because of the government's side too. A lot of our sort of assumptions in this area may be incorrect as well. The truth of the matter is we don't really know what happens behind the black box that certain authorities have access to in this area. (#10)

Adding to this fragmented perception of data access and legitimacy of requesting government actors, governments are getting increasingly creative as to how to exert force on companies to comply with their data requests. Some interviewees reported that there are police databases to compare between the disclosure practices of companies. "The police have made internal database how to request information from companies, drawing together sheets of different data to see how they are being responded to from different companies" (#14). The tactic resembles competitor blaming and can only be overcome by dedicated exchange within the industry. At the same time, this tactic of "divide and conquer" was described as being of medium efficacy, as company representatives have different views as to what another company determines is appropriate, and so the pressure by the government has limited effectiveness. To sum up, if Facebook disclosed, and Microsoft disclosed, it does not necessarily imply that Google would act in the same manner as it does not have bearing on the internal assessment. Nevertheless, a cybersecurity expert stressed that an often-underreported factor in the sensemaking to data requests is

the revolving door policy between the corporate and the public-sector staff. Personnel within telecommunications companies and platforms can either include people with prior work experience on disclosure requests for the government, or be surreptitiously infiltrated by staff with a double institutional affiliation to both the company and the government (e.g. secret service).

An important channel for data requests that were perceived as highly political in nature that was repeatedly mentioned are the Mutual Legal Assistance Treaties (MLAT, compare chapter III.). In public policy documents, among others, Google refers to an MLAT framework as well as other diplomatic arrangements when responding to data requests from foreign entities (Google, 2020). So, can non-US agencies work through the US Department of Justice to gather evidence for legitimate investigations for which agencies would like to access data from Google? Google may also provide data on a voluntary basis if the request is consistent with international norms, US law, and the law of the requesting country (Google, 2020). An international agency goes through a diplomatic process, like MLAT. Hence Google might convey the same information to a non-US agency as it would if the request originated from a US agency. In a way, company representatives perceived MLATs as a sort of protective shield in their sensemaking processes that prevents them from being sucked into legal processes. At the same time, there was a high awareness that MLATs are, to a certain extent, outdated. In the US, for instance (#14) the US department that processes MLAT requests was alleged to be a systematically defunded office at the Department of Justice, that receives too many requests and has too few people to handle them, yet nevertheless is an important intermediary on the US side of the border. A telecommunications representative described the global process of handling data requests in correspondence with the MLAT as follows:

At least with MLAT it's dealt at state-level and then referred down to us, so we at least know that it's had... that it's under the rule of law (...) that theoretically it had a state evaluation before it comes to us. Whereas if there is a direct request from a state, that we don't think that we should be the ones who have to do that evaluation process – I mean it must significantly increase the level of scrutiny that it requires. It takes away that insurance frame. (...) It also increases the complexity. At the moment the team in the UK for example has a list of agencies that they know are authorized to make requests. If suddenly a law enforcement agency in the US, or France, or somewhere, is also able to access that data, it increases the complexities as to the operations that they have to handle. (...) And it might mean that we get a request that is not in a language we are able to decipher. And also, I think that there is an increased risk that because of the extra evaluation that certain companies might just comply and therefore basic protections could fall out the window. (...) this challenges as well some of the time scales that are in the e-evidence [proposals], to disclose within 24 hours/7 days a week. Trying to evaluate that, you have lawyers on call to be able to do that I would expect, so yeah, I think that's ongoing. Lots of pushback (...) the MLAT puts the company in a much more comfortable position. (#7)

Yet interviewees also recognized that while the MLAT might offer protection from getting involved in political power struggles, it has become “antiquated” as, for example, “US companies bound by US law does not hold water anymore” (#23). It was stated, “when authorities outside the United States track data about users located outside the United States it’s just a mess, they can’t do it, the process is extremely slow” (#3). MLATs do not appear suitable for the fast-paced data ecosystem. Nevertheless, certain actors comfortably maintain that they will rely on them, stirring anger from government parties making requests.

To conclude, the overall desire for more clarity about data requests from government actors was very high through all interviews and the political transnational framework appeared to be in flux at the current moment in time. Interviewees (#28) criticized the law as requiring greater clarity, and noted that the law should not be open for interpretation in that area: Overbroad law can be interpreted in many ways; pushbacks will be harder when clarity is lacking. Civil society experts also pointed to the mixed track record on transparency efforts by companies, shifting the narrative also to the private sector duty to uphold privacy rights of their users: “the companies (...) are not doing much more than 50 in the Corporate Accountability Index of Ranking Digital Rights so there is a pretty good way for improvement in terms of disclosure transparency. This is such an opaque place” (#5).

It is worth highlighting that interviewees mentioned some country examples and geographical regions to illustrate difficult data requests by governments, yet also emphasized that there is no continuous geographical pattern overall. Also, in Europe, companies are sometimes not allowed to disclosure detailed information on their data sharing practices with the government and policies can in part be very restrictive. Whereas some Western governments might be busy pointing fingers at the global South, these same states in the southern hemisphere might just be mirroring “Western laws”, pointed out one platform representative. Given the broad geographical scope of most of the interviewed companies – with business units operating across several continents and multiple jurisdictions therein – this comparative perspective was helpful in further dismantling the terminology. The following sensemaking dimension will therefore shed light on the sensemaking process to data requests that rests heavily on the relationship with the company headquarters.

2.7. Relationship between headquarters and subsidiary

As noted in the process models in the beginning of this chapter, organizational models differ with regard to the strategic involvement of the subsidiary in responding to data requests from government actors. On the one hand, a set of the companies depict the following:

A very dynamic relationship with our local operations. We speak to them on a daily basis. And that for me is the real key here: building your trust and your relationships with the guys on the ground on a day-to-day basis. Otherwise, you know, you can make the most illustrative sort of fancy nice looking report but if the data, the underlying data is provided by someone who doesn’t really

understand what you are asking for, or doesn't really have faith or trust in the head office that they are interacting with, you have lost before you have started. So, I think the relationship between head office and local operations is absolutely paramount to being able to a) deal with these situations in a rights-respecting but also safety-conscious manner and b) provide the kind of transparency and disclosure that external parties are seeking in regard to this area. That would be my big take-away from our perspective. (#10)

On the other hand, the headquarters is the real centre of decision-making power about data requests for certain companies.

The real decision-making process is that the government is asking our local CEO, the local CEO refers to the corporate CEO of the region – we have a country CEO, a region CEO and then there is a top management here in [European city]. And when the message comes to Paris, then I am in the loop. And I do my part which is try to resist and try to communicate with civil society whereas the local CEO with the help of the corporate chief is trying to open discussion with the other telcos first and with the government when the minimum requirement, meaning a written demand, is not obtained. It's usually very fast, it's an emergency situation but we can make the reach through the whole chain of command on this issue within 24 hours. (#12)

Across both models though, establishing jurisdiction for the data request is a key factor. Apparently, for example, in the case of platforms headquartered in the US, US law is strategically applied to data requests related to users located in non-US territory but with their data being located in the US:

From the perspective of the US company, they get away with (...) They don't have to respond (...) the consequences if they don't treat them as seriously, they have lots of easy ways of denying these requests and they have a lot more freedom in the policy they set. At the moment unless there is a request through a Mutual Legal Assistance Treaty, an MLAT, or possible letters rogatory they are not going to... law enforcement officials are not going to get the consultations from responders, they will sometimes give metadata, I have been involved in a couple of cases like that. And they are largely at the moment governed by US law and so they have, you know, an easy way of filtering a lot of requests, the requests. They are very often not compliant with that law and so they can ignore them if they see that's the case. (#3)

So partly, rather than being concerned about the large multinational big players, civil society experts pointed out that (#5) local activists are talking about the challenges of engaging with smaller, local companies and are much more concerned about what local companies are handing over to governments, rather than being concerned about the big platforms. They see that the big platforms have more leverage and ability to resist than local ones. Multinational companies even in the telecommunications sector can sometimes use jurisdictional leverage to push back on requests, e.g. "So quite often we end up with a situation where we would get a

request in Thailand for example and we have to get back to the police in Thailand, saying that we provide that service to Global Services in [European city] and they obviously get quite frustrated at times, 'You're (#7), why can't you tell us?'" (#7).

Interviewees were strongly aware that in the early phases of the internet there was the belief that "the internet doesn't have jurisdiction, that was the idea" and the mantra followed "What is data? Is it actually in somebody's control?" (#16). In contrast, the nature of the fragmented global governance made it necessary to exert some degree of local responsibility. At the same time, the code on local responsibility and how to establish it was characterized by views and perceptions that concurred, broadly echoing the differences in data location models of platforms versus telecommunications companies and their difference in volatility with regard to people and infrastructure on the ground (see sensemaking dimension on organizational structures and factors). With regard to how companies try to make sense of having a cooperative relationship with the government, the local accountability model of a telecommunications company has been depicted as follows:

Identify a point of contact who is a national of those countries to give them a process to follow and just in case we get a request... We just found from experience that generally the law enforcement agencies are more comfortable when it is a local national within the local entity of (#7) that they can approach and have a conversation with (...) helps with the language issues (...) points of contacts. They are named people within the country. There's (...) what we call a front-desk process, this sits in any public facing area, like reception area or your mail room. So, that any request that looks like what we've called a law enforcement agency request (...) might be that a good reason to have somebody who is national of that country because they are familiar with "OK you got a security agency here, you got an intelligence agency" and know the names maybe (...) there are official stamps, court stamps, signatures, dates – all to build a picture of the validity of that request before proceeding. But if there are, within the process there, it can allow for, go back, pushback, refuse to comply with the request, ask more questions, ask for more information (...) we flow down policies and processes to the local level and we encourage local accountability rather than (...) a top-down approach. (#7)

Other telecommunications companies argued on similar lines of local accountability (#9, #10), whereas another set of telecommunications companies made sense of the relationship with the government relying on more group-centric action – as described below:

So that it is a formal decision how to respond to the request, if and how, and what pushback to do, is decided with the local company together with the group (...) A day to day request in each country goes to a local team and works specifically on this position. (...) also, a very basic idea with this policy was that to ease the pressure on the local company. Because often it is very difficult for local employees, citizens of the local country and national police and secret police around the corner to pushback in any way. But what they can do is to

say, “we have a policy which obliges us to escalate the issue to group”, that they can do and the policy in our procedures makes clear that decisions on such requests need to be approved on group level. So, I then coordinate helping the local company to escalate to relevant people on group level to approve how to deal with the request, including when and where possible with measures to respect the rights of users. (#8)

Adding to the two concurring models of dealing with complex government actors, civil society experts (#5) added that they saw the necessity that a company representative or at best a team looks precisely at high risk communities or those who might be suffering repercussions in terms of human rights at the hands of governments. Throughout the interviews it became clear that the major motivating factor for companies’ sensemaking in an amicable way towards an even quite repressive regime is the fear of threats to local staff. Threats to local staff by the government were perceived as a key issue, though strategies of shifting away the pressure from people on the ground differed. In particular telecommunication companies reported exfiltration measures, or their CEOs of subsidiaries being imprisoned. Again, the situation of platforms differed strongly – as described using the process models in the beginning of this chapter as well as illustrated by the following quote:

Google or Facebook, these very large internet companies, I am not sure they would say this publicly but I think the approach that they take is: when considering requests from various countries, they will consider what their assets are in those countries and whether they feel that these assets are well protected or not well protected, and that might well influence whether they respond to these requests and how they might respond to these requests. So, if they get a request from a country where they don’t have any assets on the ground, no employees or offices, it might feel more safe or secure in ignoring it because they can’t have their employees arrested or they might not get extradited to that country, if it’s a large country where they have a large presence they might be more careful because they don’t want their employees being thrown into jail. (#3)

Beside threats to staff, it is harder to push back when you have a local office with key infrastructure on the ground; that certainly counts into evaluating the assets when assessing the response to a data request.

The document analysis indicated that certain companies also provide information about the interaction between subsidiary and group. Millicom is one of the few companies that provides a little bit more detail as to how it differentiates between groups of requests and in which business units they are assessed:

Millicom’s assessment of and response to government restrictions and demands that impact the privacy and freedom of expression rights of its users is directed by its LEA-MEP. Millicom draws a distinction between two categories of requests. The first is government requests for user data, which are issued in writing by an entity authorized under local law to do so and appear

on their face to be consistent with local law and international human rights standards. Such requests are logged in a database maintained by Millicom's in-country, in-house legal team that is audited by Millicom's corporate team on an annual basis. Millicom's in-country lawyers scrutinize such requests to ensure that they comply with all applicable local legal requirements. If they do, Millicom will grant the request on the narrowest possible basis. If not, Millicom will reject the request and explain its reasons for doing so to the requesting government entity. The second category comprises all government requests and demands that are not in writing, obviously inconsistent with local law and/or international human rights norms or the terms of Millicom's operating license in that country or appear on their face to be politically motivated. These are considered "Major Events" that must be escalated to the company's executive-level personnel for review and decision. Once a Major Event is escalated to Millicom's senior personnel for their review and decision, the company evaluates the full range of available options before formulating a response. (GNI, 2020a, p. 64; Millicom, 2020)

Again, besides human rights requirements, some telecommunications companies saw their hands tied in respect of pushing back by their legal obligation to comply with any local laws that might actually be in conflict with international or regional standards. "Sometimes there are – for better or worse – local laws and license obligations which compel us to provide information to authorities that international standards or norms would actually prohibit or discourage" (#10). The latter statement leads into the broader discussion about the company mindset as the backdrop towards human rights when making sense of data requests. The following section will explore how interviewees made sense of data requests in relation to the human rights mindset of the company.

2.8. Human rights mindset

Naturally, given the interviewees' backgrounds and their institutional setting, almost all interviewees emphasized a human rights lens as a backdrop to the sensemaking. The extent that translated into actual practice differed, with some companies clearly committing to "to resist demands, and refuse, and whatever we are able to serve" (#6). In particular, privacy and freedom of expression were a focus (#10). Some platforms compared dealing with a data disclosure requests as a "well-exercised muscle" (#23), characterized by greater knowledge as in other areas: the process was described as involving the executive level, and the team level with managers that have long embodied these human rights values, and a high level of awareness among the staff who deal with these issues. Other companies, predominantly telecommunications companies, when dealing with data disclosure requests, described their mindset as being rather on a journey to a systemic understanding of human rights impacts, and saw themselves as very limited in their scope of action by the license agreements. For instance, (#28), there would be a special triage for human rights incorporated into the standard triage for data requests to include human rights elements, but the employees (security team) who are processing these requests would not necessarily be human rights specialists.

Human rights due diligence

As part of this journey, human rights due diligence was mentioned in various forms – such as telecommunications companies when (re-)negotiating license agreements with local governments (#1) or moving their business into the 5G space, based on human rights due diligence requirements (#12). Some companies had human rights due diligence panels in place to approve the sale of their products (#25) and in particular telecommunications companies moved towards conducting human rights impact assessments, e.g. for specific markets with re-occurring issues or for market entries. Such assessments were made in cooperation with 10-15 interviews local staff that managers based in the headquarter described as very fruitful, because on many occasions the people working with human rights locally said: “oh this is the first time that we get to meet the telco, any telco in this country, we were able to meet” (#18). Ideally, representatives hoped that through such measures could build interactive networks between local staff and people worked on transborder issues in the headquarter. Generally speaking, whilst many companies endorsed a human rights lens, the implementation across the business units was fragmented at times for some telecommunications companies. These companies also recognized that “we had [consultancy firm] to conduct a really thorough human rights impact assessment for (country x) (...) we do also acknowledge that that’s something that might have happened a little bit too much on an ad hoc basis.” (#25). Others already had dedicated teams, training and assessments for human rights in place.

Setting the default as actively rights-respecting

Among the more surprising, proactive moves of some platforms was the re-framing of requests and/or labelling of metadata as content (compare sensemaking dimension on routine process for unusual requests). This is an example of when progressive company practice goes towards setting rights-respecting practice as the default. Location data was seen as content for some platforms and perceived as not legitimately authorized for government access (compare also to the sensemaking dimension on routine processes for dealing with an unusual request). Adding to this, even the blaming strategies described in the sensemaking dimension about the government relationship when the government tries to stifle competition among corporate responses to data requests was more or less seen as irrelevant for the internal sensemaking process about data requests. A rights-respecting human rights mindset would still draw the line at their previously set default stance towards a progressive rights-respecting practice. This included the perception that the companies looked at the data requests from the privacy perspective of their users, which came up with a handful of interviewees, such as in the following example:

So, companies are kind of putting them in the shoes of the users, raising their users rights (...), particularly when the requests seem extremely broad or don’t have a valid basis – in suspicion or something like that we might be raising these kind of arguments. So, in terms of a request that implicates the accounts

of lots of users and implicates lots and lots of data we might be making that kind of objection. (#3)

Juxtaposing business environment and human rights practice

Certain telecommunications companies, more exposed to the goodwill of the local host government, described how they see a market entry as a key point for carrying out due diligence as the first engagement on the overall government relationship, and then continue case-by-case (#12). They perceived a market exit as a difficult decision to take.

On top of that is the question, would you leave a country, or would you not go in a country if they would not respect your due diligence requirement? And the answer is mostly no because we are so much involved in human rights issues so that we are probably the best candidate to try to make the country change than just let someone who doesn't care about it, settle. (#6)

Interestingly, there was also hidden criticism from telecommunications companies towards platforms with regard to data use "we will not use the customer data, again we are very different from internet companies that do make their business on customer data – we do not" (#6). Data minimization – collecting and storing as little as possible, so the data is not there in the first place – did not come up in the interviews with corporate experts and was a minority civil society opinion: "there is some tension there and some tricky issues but for the most, you know, companies are, generally companies are much too quick to over-collect, to over-process and monetize data" (#5). Also, only one corporate interviewee described remedial measures for users:

We have a very strong remedy process in which we prioritize of course our customer to offer them compensation for whatever they have lost. So again, it's an existing process and I am trying to grab this process and to make it bigger and to have remedy issues when it comes to network shutdowns or when it comes to data privacy issues. The discussion of which is now very vivid between the company and the government within our engagement with them is of course many times what is happening is not our action. (#6)

Despite not being fully anchored in their practices yet (see sensemaking dimension about organizational structures and factors) interviewees stress the necessity of engaging in the long-term with external stakeholders and becoming publicly vocal for a rights-respecting business environment.

We are using our merger into the civil society, to human rights defenders and I am carrying with the GNI and all the different session (...) to have a civil society to help us in some cases where the demand is completely out of the record and in which the (...) publication from NGOs or any kind of civil society organization to point out the fact that this is not the right way to do, this is also something that we are trying to use. This is not governance, but it is definitely

a way to defend our side when it is not too difficult or too dangerous. (...) Again it's this thing can you engage in the moment when you are faced with a particular situation or more broadly and generically, but not necessarily in the moment. (#12)

Others described that the company made a statement that they cannot comply with local legislation that is in contradiction with the European Charter, according to the European Court of Justice and they "don't apply that national law but that is a difficult standpoint, too, to stand up to" (#18). Also, civil society recognizes that nobody is "supreme relative to the law of the land" but that there "should at least be (...) a lot of pushback before the information is handed over. Many of these companies (...) have their operations in the global North, in terms of headquarters that have friendly laws or at least respect privacy – so maybe there is wasted advantage of that" (#4). This notion corresponds and is mirrored in some of the actual company practice described by a telecommunications representative as follows:

We have a policy which obliges us to escalate the issue to group (...) the policy in our procedures makes clear that decisions on such requests need to be approved on group level. So, I then coordinate (...) helping the local company (...) then it's escalated to relevant people on group level to approve how to deal with the request, including when and where possible with measures to respect the rights of users. (#8)

To summarise, a thorough basis of triangulated qualitative data has allowed for an exploration of the black box of data disclosure requests by shedding light on the corporate sensemaking process when responding to such requests. The following chapter will discuss how the findings relate to various strings in the current academic debate around sensemaking, managing human rights across jurisdictions and the state-business nexus.

VI. Discussion

This research set out to explore a specific lacuna in the data economy: the phenomenon of black boxes manifested in the example of data disclosure requests from governments to companies. The aim was to examine how companies respond to governments' requests for user data, from a B&HR perspective. The ability of having access to the field, at times, was challenging (see section "access to the field"). Of greater value then are the insights obtained based on the interview data for the scholars interested in this field of research. Relying on the triangulation of policy documents and expert interviews, the data analysis revealed key patterns in which companies try to make sense of government data requests.

The research provides scope to open and explore the black box of data disclosure requests. The findings allow for insights and to construct what was previously a hidden process. Overall, the findings demonstrate that companies now have taken a look to human rights to inform their management practices when responding to requests for user data from governments, as reflected in the sensemaking along the three dimensions proposed by the literature: organizational factors, shared understanding in the organization, and early actions taken in crisis (Weick et al., 2005). This constitutes new insights for the B&HR scholarship on the implementation of human rights in business practice. Applying human rights serves as a novel standard that works above national regulation to mainstream rights-respecting practices when responding to atypical data disclosure requests across countries. Nevertheless, the sensemaking process also showed the emergence of an additional five dimensions that are necessary for constructing how companies are responding to government requests for user data. These are as follows: external environment, routine for unusual requests, government relationship and headquarter-subsidary relationship, in addition to the human rights mindset (compare IV. 2). There might be a natural tendency among the interview participants to embrace a systematic human rights-based approach to assess data disclosure requests. It might reasonably be inferred that companies with less human rights practice in their managerial processes were perhaps not willing to serve as participants in the expert interviews. The interview participants included in the sample might have a natural inclination to argue based on human rights language. The findings also depict that human rights as a novel standard above national regulation can lead to frictions in the context of the external environment, and/or with local governments (see "government relationship").

1. Moving from sensemaking to sensegiving: "normalizing the unusual"

The majority of companies described how they had strategically moved towards a multi-disciplinary, rights-based approach for assessing data disclosure requests and how they anchored higher awareness and increased organizational capacity through mainstreaming, and in different ways following different strategies. To a certain extent, a known and anticipated bias in the data was that the participants represented rather mature actors in the field. Nevertheless, even these mature actors reported a

considerable frequency of crisis moments when dealing with data disclosure requests, and re-occurring elements of surprise in high-risk markets. The findings point to the fact that the emergency situation narrative has become relatively established and that the sensemaking process has started to move away from a crisis response to a more proactive sensegiving approach (see chapter IV. 1.). While in sensegiving the emphasis rests on attempting to influence other people to perceive and interpret certain actions and events in particular ways to initiate strategic change, sensemaking usually precedes this when an organization and its actors are confronted with somewhat surprising events, like crisis moments, and have to first orientate themselves and construct a new meaning for the situation they find themselves in (Gioia & Chittipeddi, 1991).

The findings also allow us to explore the question of what triggered the shift from sensemaking to sensegiving for certain companies: what is the role of stakeholder exposure and stakeholder power in companies' turn to alternative forms of managing requests? Earlier scholarship by Maitlis and Lawrence (2007, p. 65ff.) found empirical evidence of two main reasons triggering a sensegiving process. On the one hand, sensegiving was shown to be associated with the perception by stakeholders that an issue was important to themselves, to their stakeholder group, or to their organization as a whole. This can be broken down further into the perception that the issue affected the organization's performance or viability, or that the issue affected stakeholders on a daily basis in their experience of work, or that the issue affected stakeholders' compensation or security (Maitlis & Lawrence, 2007). On the other hand, sensegiving could also be triggered by a perception of a lack of leader competence regarding a certain issue. A lack of leader competence relates to stakeholder perceptions of poor organizational decision processes and poor outcomes of leader decision-making or lack of leader expertise (Maitlis & Lawrence, 2007).

There are some interesting clues here related to the interview material. First, adverse impacts of responding to a data disclosure process were certainly perceived as an important issue to both the stakeholder group and the organization as a whole among interview participants. For the telecommunications representatives the security element for their staff came out strongly as a major concern when responding to data disclosure requests. Examining the telco licensing agreements and/or related obligations in this regard provided insights on how responding to user data requests is a mandatory obligation for telecommunications companies as critical infrastructure providers, and this to some extent can dictate the requirements on the internal processing of these requests, e.g. limiting the access to this information internally to designated staff with security clearance. This is most often dictated by local regulation and authority requirements, and also limits in many cases the possibilities of group involvement in the request handling process. This again testifies to the need for the company to move towards sensegiving in order to have robust processes and safeguarding mechanisms in place in each operating market. Second, historic mishandlings and their repercussions on human rights have resulted in a perception of a lack of leader competence regarding the assessment of human rights impacts of data handovers and, in particular in the case of Yahoo!, this had initiated a sensegiving process, as several interview participants described. Another interview

participant pointed to a corruption case involving a regional unit that triggered a wider organizational response in mainstreaming risk assessment procedures, and constructed shared understanding in the organization about how to deal with unusual data disclosure requests.

Despite the fact that many companies appear to be moving to a sensegiving process and shifting towards a human rights-based approach, major events related to data disclosure requests were still seen as a trigger for crisis response – but on a stronger institutionalized human rights foothold (see “organizational factors”). Overall, the findings signal a hybrid process moving from sensemaking to sensegiving for the “routine unusual requests”, whereas some crisis moments triggering the sensemaking, as a crisis response mode, persist. Important clues can be drawn here in the response from a range of platforms and telecommunications companies when confronted with increased government demand for user data in the initial response to the COVID-19 pandemic in spring 2020: the deviation from the “new normal”, that used to cover previous routine response, and the pandemic hitting novel triggers. The scale and scope was beyond what data-intensive businesses were asked to share before, and companies and governments had to reach an understanding of which user data is acceptable to share, in which format, and with what limits. For example, Apple has publicly described how the global outbreak of COVID-19 had swiftly resulted in increased cooperation with governments, and highlighted the central importance of strong privacy and data protection safeguards to ensure user trust in rights-respecting data governance, and by that increase the efficacy of tech-based solutions in fighting the pandemic (B-Tech, 2020). Further, Apple emphasized the necessity of data minimization, ensuring basic data protection and privacy principles while still being able to provide for effective contact-tracing through decentralized systems (B-Tech, 2020). Similarly, Vodafone has publicly communicated that it shared metadata to enable governments to observe patterns of movements, but no further granularity on the individual user level (Vodafone, 2020). In practice, such a hybrid model might involve a combinatory logic of sensemaking and sensegiving within the same company. Certain cases might not trigger surprise within the organization and are manageable following a routine procedure of “formality requirements” and normalizing “the unusual” with a mainstreamed assessment of the scope from a human rights lens (see “routine for unusual requests”). Such sensegiving additionally might build onto a shared understanding in the organization that thoroughly assesses unusual requests against the backdrop of the UNGPs. This is important to the organization as a whole, and can shield staff and rights holders on the ground from harm. Other cases within the same company might still trigger a sensemaking process when the government uses new tactics and/or a request shows an element of surprise, provoking the need for the organization to come up with a case-specific, novel response (see “early actions taking in a moment of crisis”). Where such cases constitute a crisis moment, the shared understanding might resemble a contested terrain, as internal communications might require a very close exchange between the subsidiary and the headquarters about the situation on the ground for the specific case, whereas external communications could strive to hold onto maintaining ambiguity in public relations (see “shared understanding”). How these conclusions connect to the dominant themes in the B&HR literature will be discussed in the

following section, in particular building on the notion of a combinatory logic of sensegiving and sensemaking.

2. Lifting the corporate veil? Combining local accountability and protection at the group level to respond to complex situations

Traditionally, the B&HR discourse starts from a line of argumentation as to why companies have the responsibility to respect human rights, why the state duty to protect human rights needs to be amended with this corporate responsibility, and how remedies contribute to fulfilment (Obara, 2017, p. 270). Among the interviewed participants, companies did not perceive the government as fulfilling its duty as a human rights bearer, partly given their negative experiences dealing with governments. On the contrary, many companies perceived the state as a “perpetrator” or “facilitator” of privacy violations and connected human rights harms when requesting data in overly broad, inappropriate and/or threatening ways. As a reaction, several companies described how they aim to protect rights holders by ensuring a regular and systematic exchange with business units in affected regions. In order to shield potential victims from a harm occurring, they aim at “lifting the corporate veil” between business units: the governance and management structure are adapted to allow for as close communication as possible, and/or permitted by the law and, by that, enforce their corporate responsibility to respect human rights when responding to data disclosure requests. Human rights experts charged with mainstreaming the response patterns to data disclosure requests reach out proactively to business units to raise awareness and train their subsidiaries on best practices in responding to unusual requests so as to avoid it escalating into a crisis. In crisis moments, then, it appears that many companies work with an internal taskforce to mitigate harm, and if necessary, loop in external stakeholders that can support in directing harm away from staff on the ground or the people whose user data is the object of the request. To a certain extent, this reverses the claim of a swathe of companies that argue that they only have limited control over their foreign subsidiaries, insisting that the legal framework does not require enforcement of their managerial responsibility for respecting human rights down to the local level (Kobrin, 2009; Matheson, 2008; Ruggie, 2014; Skinner, 2015). On the contrary, the interview material demonstrates that the exchange between headquarter and subsidiary is extremely close and of major strategic importance when dealing with data disclosure requests.

Companies rely on two differing response models for the most part: (a) the headquarter has a protective function towards the subsidiary for some companies and/or (b) local responsibility with the aim of increasing local legitimacy and using local expertise. Nevertheless, the fragmented governance between different jurisdictions remains complex (see “external environment” and “government relationship”) and this might be why the framing and language matters, and why companies sometimes also combine local accountability with group protection if the specific situation requires it. By adopting a clear use of human rights language and

moving towards such use across departments, companies may signal the very political nature of the requests. The implications for rights holders could be positive if the corporate measures evolving from the close coordination between headquarter and subsidiaries are aligned with a rights-respecting framework – ideally the UNGPs. For example, if a company mainstreams their assessment process of government requests for user data across all its subsidiaries, and makes this process public, this helps rights holders to better understand how they can engage with the company to raise concerns about potential government surveillance tactics. It appears that the publicly available assessment sheet by Telia Company can be a helpful illustrative tool for such purposes.

Further implications from a rights holder perspective lay in the space for cooperation that this close linkage of corporate decision-making offers with regard to cooperation between the home state and technology company to deal with the heightened risk of gross human rights abuses in conflict-affected areas – called for by UNGP 7 (UN Human Rights UN, 2011). Here, host states can ensure that technology companies operating in those contexts are not involved with such abuses, if they work closely with technology companies domiciled in their jurisdictions. As the research shows, technology companies are able to govern and manage data requests at the nation state level in a host state – and here lies an important lever with regard to the foreign affairs of the home state of a technology company. Measures in line with UNGP 7 should include engaging at the earliest stage possible with technology businesses to help identify, prevent and mitigate the human rights-related risks that stem from their digital technology products, services and business relationships; providing adequate assistance to technology companies to assess and address the heightened risks of abuses, paying special attention to both gender-based and sexual violence; denying access to public support and services for a technology company that is involved with gross human rights abuses and refuses to cooperate in addressing the situation; and ensuring that their current policies, legislation, regulations and enforcement measures are effective in addressing the risk of technology companies' involvement in gross human rights abuses.

At the same time, the inherent normative conflict in internet governance identified by Flonk et al. (2020) was portrayed in most interviews as a huge impediment in finding common ground for transnational management practices with regard to data disclosure requests (see chapter I. 4.2.). This is also echoed in respect of the frictions around data disclosure requests as these reveal the inherent tension between the state duty to protect human rights and the corporate responsibility to respect human rights in the UNGPs with regard to the rights of the data subject (see chapter I. 4.1.). The findings (“government relationship”, “internal communications” under “organizational factors”) have illustrated how the relationship between the state and companies when dealing with data disclosure requests is characterized by structural opacity. This structural opacity derives from what comes across as a closed-door relationship between corporate executive management and state actors in the requesting government departments. This opacity implies a lack of public scrutiny: when the key conversations are predominantly taking place behind closed doors, the public cannot meaningfully deliberate the boundaries and objectives of data sharing

between the private and the public sector. Further, it also strongly hinders mutual learning within the technology sector as companies cannot communicate in a detailed and nuanced manner about evolving issues of data requests from government parties in particular states. To a certain extent this arrangement between state and private actors is the result of issues of policy coherence. The transnational policies of data sharing between private actors and state are not coherently regulated, opening up a range of loopholes which states can use for their advantage when they want to access user data. The national security/emergency narrative is, according to the interviewees, one of the key motivations for states to use such loopholes or draft regulation to broaden government access. Consequently, the systemic risks for rights holders stemming from a fragmented and inconsistent global framework for data disclosure requests are high. When states overstretch the security narrative with regard to data disclosure requests, they do not live up to their human rights obligations. The salience of risks to rights holders based on the information gathered from data handovers increases in fragile states, post-conflict and conflict settings (see e.g. UNGP 7). This has particularly severe implications on human rights when the government aims to access the data of vulnerable people, such as those fleeing from conflict zones.

Yet, the findings also show that certain companies proactively seek to fill the void when a nation state fails to live up to its human rights obligations (see sensemaking dimension of “Human rights mindset”, in particular “Setting default to rights respecting”). At the very least, this can be seen by the fact that most of the companies coherently check the formality requirements when a request comes in and are moving towards a rights-respecting assessment of requests, and are thus slowly moving beyond pure legal compliance assessments (see chapter III. 3.2.). The recent cases in Hong Kong, where several tech companies decided to halt cooperation with local authorities on data requests, and the requests to Facebook with regard to the case filed by The Gambia against Myanmar at the International Court of Justice, both illustrate the need for a renewed assessment of each situation (see Chapter II.) (Hern, 2020 ; Z. Whittaker, 2020). In a way, the case in respect of The Gambia needs to be seen in light of the fact that the same kind of requests have been used and continue to be used against human rights defenders in many instances. What is observable in Facebook’s public reaction when assessing that very request – and the company coming to the conclusion that the scope of the request is too vague and broad – echoes very strongly with the findings on the routine process to evaluate requests (“formality requirements”). For the rights holders this has important implications. When companies, through their external media work, shift the “secrecy” of data disclosure requests into the public spotlight, it can empower human rights advocates in their work and raise levels of awareness as well as public scrutiny of government conduct around data requests. On similar lines, it can also warn human rights advocates of increased government appetite in user data, so that potentially targeted individuals can tactically upscale their measures for protecting their data.

The element of public communications is interesting to explore further in light of the findings. It relates to how much the company can communicate in public about its actual human rights practices and will be discussed in the following section.

3. How the state-business nexus limits genuine public communications and hinders assessment of whether companies “walk the talk”

It appears that many companies are moving towards turning an anticipatory risk assessment lens on potential adverse impacts on human rights in order to minimize harm by taking a human rights mindset. Interviewees highlighted how they raise awareness, mainstream training measures and align hiring policies to get as much in-house experience for a multi-disciplinary assessment of data disclosure requests as possible in using an UNGP-oriented lens. Adding to this, a handful of telecommunications company participants sketched how they are slowly starting to carry out human rights due diligence when entering into license agreements with states, or assessing existing license agreements from a human rights due diligence perspective. This relates quite well to the introductory example of Authority Requests to Telenor, which highlights how Telenor proactively spotted a gap in the regulatory approach in local law for data disclosure requests and entered into dialogue with the local government to close that gap.

Nevertheless, the findings also highlighted the inherent tensions between the limitations laid upon public communications by companies to transparently report what is happening inside companies (“external communications”) and the lived human rights mindset of companies (“internal communications” under “organizational factors”, “human rights mindset”). Even when companies had a progressive human rights mindset and matching internal communications processes, their sensemaking reflected that they feel extremely limited by law to engage with external stakeholders on actual requests or communicate publicly in a meaningful way about it. Such findings are also relevant in light of the research by Jørgensen (Jørgensen, 2017, 2018) on the framing and storytelling of human rights in tech companies. Jørgensen (2017, p. 292) argues that while the platforms like to use rights-respecting metaphors connected to rightsholder's ability to exercise rights, in fact companies also enjoy taking liberty to determine the room for interpretation of these rights and enforce their own rules of engagement. Also in the context of data disclosure requests, companies might strategically use opacity to set the agenda in the most beneficial way to their governance structures, as they move to sensegiving rather than sensemaking as a crisis response.

This needs to be seen in the context of the strong dependency of the government on the data collection efforts in the private sector and the fairly limited ability of the government to collect comparable amounts and quality of data (Howard, 2015; Mazzucato, 2011). In practice, it might force the government to access data from the corporate sector and raises fundamental questions about the nature of democratic governance: do we wish private companies to be the repositories of our data, or do we prefer to have the data in the government's hands, arguing that there are sufficient means to hold the government to account? Future research could also investigate the different government departments and their (non-)alignment with regard to data policies and practices. Such research could investigate whether human rights

departments in governments have a say about the data access policies of security services, and whether their say is really taken into account or is more a fig-leaf consultation. The research might also shed light on the question of whether governments are actually aligning their requesting tactics between departments from a strategic perspective, including potentially red flags, or if evaluations emerge on an ad hoc basis when a legal process requests additional evidence. Relatedly, within the state-business nexus, this strengthens the notion around adequate oversight to ensure states meet their human rights obligations when requesting data and providing the sort of transparency that is demanded from companies (Parsons, 2019; Soghoian, 2011).

VII. Recommendations for progressive conduct

To move on from the struggles of a microcosm in a larger crisis in contemporary governance (Ruggie, 2014, p. 6) (compare III.4.4.), the findings clearly demonstrate that companies alone cannot solve the puzzle of finding a more rights-respecting approach to govern data sharing practices between the state and the private sector. The research scope afforded a better understanding of the organizational processes of companies' response to unusual data requests by government. It permits learning as to how companies in the technology sector implement B&HR to align and improve governance in complex environments, and further demonstrates that the human rights framework is fit for purpose to be used in this space and to inform new global governance models on the business-state nexus. Companies should be congratulated for having moved toward a human rights-based approach to decision-making about data disclosure requests, though there clearly remains room for improvement for aligning and further substantiating efforts to create a level playing field of practice. Novel cross-border cooperation rooted in a human rights-based *modus operandi* needs to rely on building blocks, such as the "Necessary and Proportionate Principles" (EFF, 2014) that advocate for better rights protection – specifically in communications surveillance – as well as the UNGPs (UNHRC 2011) for finding the right way to involve the private sector and engage their corporate responsibility to respect human rights, ideally building on a "thick stakeholder consensus" (Pauwelyn et al., 2014) (see elaborations in chapter III.4.4.). This could entail the development of better transnational norms for data disclosure requests through testing cooperative models in emerging cases and allow for the building of novel alliances across building blocks. It would ultimately allow for the area of data disclosures to re-emerge out of "real secrecy", "legal secrecy" and "obfuscation" (Pasquale, 2015, p. 3) as a matter of public concern that should be discussed in a deliberative process to avoid an erosion of democratic forms of governance (Habermas, 1995). The following recommendations connect to the findings and aim at making a contribution to move towards a rights-respecting norm based on a thick stakeholder consensus for responding to data disclosure requests.

1. Governments - Enable companies to provide transparency in meaningful ways

A challenge persists in the fact that technology developments are currently outpacing regulation and policies, which risks continuously leading to patchy or overlapping regulatory and/or policy frameworks that are not properly founded in states' human rights obligations. Nevertheless, as the discussion in chapter II has shown and in light of the findings, better policy can only be drafted when informed by reliable information on the scale and scope of the data sphere in the state-business nexus (see Chapter II.). Therefore, governments need to enable companies to provide transparency in meaningful ways. Establishing ways in which companies can be transparent about the sheer scale and scope of cross-border data sharing from companies to governments is essential. This could also involve increasing transparency to users about how long government requests, including personal information provided by governments in the request, are retained by the company (GNI, 2020a, p. 96f), and broaden the scope of when notification of users is permitted by law.

Key ideas as to how governments can enable companies to provide better transparency reporting have already been brought forward by the literature (Parsons, 2019; Rahman, 2016; Soghoian, 2011). The findings illustrate how such calls have until today still not yet been sufficiently implemented by states in practice, despite strong calls from both industry (GNI, 2020a) and civil society (RDR, 2019). The findings have shown that the limits put on companies about publicly communicating on their practices in dealing with data disclosure requests lead to tensions between internal communications and external communications and hinder assessment of whether companies actually do live up to their human rights commitments (see VI.3.). Government should complement the picture by committing to improved government transparency reporting on government communications surveillance, and allowing government agencies to be "scrutinized" as they "scrutinize" others (Pasquale, 2015, p. 3). Overall, an emphasis needs to be placed on guaranteeing greater granularity in transparency reporting. This needs to permit companies to provide information on a) how different legal justifications are used by different agencies around the globe, b) which type of data they are asking for, c) the permitted use(s) for information obtained through a request (for instance, disclosing in criminal trials how information was obtained) and d) facilitate ways of making this information more accessible, such as by centralized reporting on a joint website for the key companies per country (Rahman, 2016).

In combination with providing greater granularity, transparency reporting should be standardized by regulators to allow for better comparability across companies, and ideally, at some stage, countries (Parsons, 2019). Through enabling companies to provide a better foundation for providing information, the scale and scope of data disclosure requests – in particular those of an unconventional, transnational nature – can be leveraged to better crystallize key human rights issues and inform policy-makers to close gaps in patchy, fragmented frameworks, and to protect rights holders on the ground.

To achieve greater policy coherence and adequately assist business enterprises in conflict zones or other situations of heightened risks, the home states of technology companies should: foster closer cooperation among their development assistance agencies, foreign and trade ministries, and export finance institutions in their capitals and within their embassies, as well as between these agencies and host government actors; develop early-warning indicators to alert government agencies and business enterprises to problems; and attach appropriate consequences to any failure by enterprises to cooperate in these contexts, including by denying or withdrawing existing public support or services, or where that is not possible, denying their future provision.

2. Companies - Align the handling of data requests across jurisdictions

A jointly aligned and, to a certain extent, standardized way as to how companies should handle data requests across jurisdictions could establish a level playing field of good practice within the state-business nexus. The findings have shown that the group or headquarters level are capable of reaching through to their subsidiaries when it comes to data disclosure requests (see VI. 2.). Through this proximity in management across business units and geographies, companies have a strong potential to align the handling of data requests across jurisdictions. Operational recommendations based on the findings for companies handling requests should include the following measures:

1) Procedural requirements relate to the moment when a request comes in at the local level. First, the company should verify the formality requirements (see V.1.): a) Is it a written demand? b) Has it been received at the contact designated to the government? c) Is it issued by the legitimate authority? d) Does it refer to applicable law? If the answer to all these questions is “yes”, the company can proceed to assess the actual scope of the request in a second step. This assessment of the scope should be done from a UNGP perspective, with an emphasis on the potential important human rights risks to rights holders on the ground. A “healthy suspicion” towards a case-by-case analysis with respect to the political context and to organizational embeddedness is key.

2) Overall governance structures should guarantee that there is a candid exchange between the headquarters and the subsidiaries (see V.2.7) on data sharing practices, and as much alignment as possible with regard to organizational structures (see V.2.2.), such as data location, documentation, and accessibility, as well as staff policy to reduce vulnerability of staff to surprise requests and external stakeholder engagement. This will potentially allow for a rapid response to avoid moments of crisis and a clearly defined ex-ante chain of response. Such aligned organizational formats could enable a move towards a shared understanding by mainstreaming a human rights-based approach to data disclosure requests.

3) To construct a shared understanding in the organization across departments and business units (see V.2.3.), the company should set up management processes grounded in a policy commitment that builds on the formality requirements and a code of conduct for assessing the scope of a request. This should be drafted as a multi-disciplinary, cross-departmental effort and could for example be conceived on the basis of the “Necessary & Proportionate” principles offering specific guidance on communications surveillance in combination with the UNGPs.

4) Shifting the default position to rights-respecting in the long-term (see V.2.8), the expansion of strategic partnerships with civil society, and, if applicable, regional and local actors, to understand the multi-centric state-business nexus on the ground is key. Inter-disciplinary exchanges, including with rights holders in various geographies, to deal with the continuous patterns of a national emergency narrative are essential – potentially allowing for a shift in the narrative on the company side, such as strategically labeling metadata as content. For some crisis moments, active resistance will be necessary, which can be more fruitful when grounded in reliable multi-stakeholder alliances.

In an ideal world, this would all involve a bold shift of powers, where companies (particularly the more dominant players in their markets) could force governments across the globe to issue requests in a format that corresponds to a good standard of practice, knowing that if governments where to not do so, their chances of obtaining the data would be low. There is a chance that such tactics would work in practice, as the actual political power of companies in certain jurisdictions is greater than that of the government with regard to the handling of data (see Chapter II.). By no means should this imply a corporate capture of the data sphere in these jurisdictions. Rather, if a critical mass of dominant players in the market were to align their default position to be rights-respecting when dealing with data disclosure requests (based on the presented operative recommendations), it would establish a level playing field of company conduct when communicating with governments on data disclosure requests.

3. Companies and civil society - Establish an emergency response coordination mechanism

Recognizing the situation in fragile state settings around access to user data, companies and civil society should work together to establish an inter-organizational and multi-disciplinary emergency response mechanism with regard to data access requests. Private governance is furnishing criticism, yet in the current state of affairs it is necessary to shield rights holders from harm. It can be a pragmatic solution in areas of limited statehood or in fragile states. Companies and civil society might be in a better position in such external environments (see V.2.1.) and in difficult government relationships (see V.2.6) to ensure respect for human rights. Such mechanisms would need to rely on a trusted network of progressive voices in this space, and aim at establishing a coordinated response process to leverage protection for vulnerable people. The strategic involvement of civil society actors would act as a counterweight against too much reliance on companies' goodwill and

provide for enhanced scrutiny when assessing cases after they have been resolved. Orientation for the precise institutional framework could be deduced from the existing literature on multi-stakeholder governance mechanisms (Baumann-Pauly & Nolan, 2016, p. 112).

This recommendation builds on the findings from the interview data that showed that companies and civil society already work together on cases on an ad hoc basis, partly facilitated by multi-stakeholder platforms such as the GNI, and see high value in such cooperative relationship building. In addition, a stronger institutional set-up would allow for better coordination, documentation and the identification of best practices while being able to guarantee a balanced representation of voices. With regard to precise ways of institutionalizing such a mechanism, such institutionalization needs to guarantee that the emergency response coordination can work in a fast and efficient manner. The aim would be to have a non-judicial grievance mechanism that enters into effect when a threat to human rights is imminent, but before the actual harm has occurred. In this regard it would not be anticipatory, but would rather allow for the prevention or mitigation of harm in a concrete situation constituting a salient threat to the rights of an individual. This emergency response coordination would work based on a critical mass in a multi-stakeholder collaboration and would need to be balanced against conflicts of interests by a diverse oversight committee and/or advisory board that would also examine the past responses of the mechanism and allow for learning by the peer group. An integration of such a mechanism within the auspices of the GNI (e.g. tying into the GNI implementation guidelines) or a UN body is imaginable. First and foremost, the mechanism requires an impartial governing body, so that it avoids being frozen by conflicting interests of members.

Such emergency coordination mechanisms should be informed by the critique of “data universalism” (Milan & Treré, 2019) and “data colonialism” (Couldry & Mejias, 2019) in the governance of data sharing practices from “western” headquarters, while potentially managing impacts occurring in the global South (Kotliar, 2020) and raising the question of which voices are incorporated, and for whom they are speaking (Mennicken & Espeland, 2019, p. 232). The research also highlighted that human rights issues around data disclosure requests are by no means limited to authoritarian regimes and/or to the global South, but rather can be a systemic issue in liberal democracies and/or the global North as well. In particular, the complexity of issues when governments balance rights against each other is highly visible in the area of counterterrorism, and with regard to the national security context (Grabenwarter, 2014).

This is why a key feature should be that of dedicated accountability: opening the black box of data disclosure requests, in order to move away from secrecy, towards a more transparent and interactive mode. Bearing in mind the time-sensitive nature of some requests, a digital platform to coordinate leverage among civil society and companies and deliver speedier communications could be envisaged, whilst at the same time allowing for tracking and reporting – including necessary follow-up. Such a platform could also be used to safeguard business-sensitive information and provide for only the extraction of the type of information that the stakeholders would need for their

decision-making in critical crisis moments. Using the leverage of the critical mass of stakeholders, the result of the coordination mechanism could, for example, be the joint denial of an overly broad request, or a joint agreement to demand the narrowing of a request. Building on the findings that demonstrate the value of ad hoc, closed-door coordination among key stakeholders in varying settings, such an established mechanism would allow for better accountability and transparency while also protecting business interests and shielding rights holders from harm on the ground.

VIII. Conclusion

The objective of the thesis was to shine light on the space for manoeuvre companies have to react to unusual data disclosure requests from governments, and how their patterns of response differ. The analysis has opened up the black box of corporate decision-making on data disclosure requests and allowed for an understanding of how companies approach such sensitive situations, with an emphasis on human rights considerations. By that, the analysis provides an enhanced comprehension of the closed-door dynamics, and can form a basis for further theorizing and research, allowing for more public scrutiny about the scale and scope of these requests and their patchy regulatory framework. This chapter reflects on methods, theory and findings, and identifies areas for future research and an outlook on developments in the coming years.

The thesis benefits from insightful, candid conversations after trust was achieved with interview partners. The research was also able to shine a light on an area of interest that is not solely explainable in statistical terms or related metrics, and that is often used in transparency reporting (Parsons, 2019; Soghoian, 2011). Instead, the objective of the thesis required a more nuanced method to grasp its complex nature. By using a sensemaking method to analyze the interviews, I was able to gather and extract information about the organizational thinking and action around data disclosure requests that would not have been possible to gather through an ethnography, participant-observation or similar contextual methods. Sensemaking (Weick, 1988; Weick & Sutcliffe, 2001; Weick et al., 2005) allowed for a better understanding of how human rights emerge as an ethical baseline for dealing with data disclosure requests from governments and for a retracing of how it has become organically embedded in decision-making processes, such as in crisis moments. The expert interviews enabled the extraction of important information from how key stakeholders spoke openly about their experience, without positioning their individual perspective as driving the company's particular plan, policy or decision; they provide insight into a phenomenon of great importance and urgency in internet governance. At the same time, the sensemaking dimensions also indicate a strong multi-dimensionality of finding better ways to deal with government data disclosure requests, for which a further analysis with a complementary method would be helpful. A method that can sufficiently address networked effects in the multi-dimensional space of internet governance (see also "thick stakeholder consensus") could build on the findings (Zevenbergen et al., 2015). One could think here of the likes of Actor-Network-Theory (Latour, 2005). When states fail to address heightened risks in conflict affected areas, impacts from the use of digital technology on human rights can be profound, and the stake that an individual business holds in a networked set-up is certainly key. Yet, alongside the role of a single nation state, it is not the only stake that can improve the protection of human rights. The sensemaking method chosen focusses on corporate sensemaking and by that naturally was not able to address the effects of the broader network's constellation. Actor-networks are understood as networks of actors – such as people, research evidence, technologies, financial resources, institutions – which act together to produce particular effects, and existing research has considered the non-human in relation to technology (Castells, 2012). A

study based on Actor-Network-Theory could build on the insights of this thesis and further substantiate knowledge by identifying key nodal or salient points in the network to consider human rights as an ethical baseline of internet governance, beyond individual corporates or single nation states (e.g. with other human actors like civil society organizations or the home states of technology companies) but also non-human actors like standardization and/or regulation on transparency reporting.

Further, the formality and transparency that the findings call for create tension with the greater contextual flexibility that many data activists and critical data studies approaches call for when studying the social impacts of technology (boyd & Crawford, 2012; Neff, Tanweer, Fiore-Gartland, & Osburn, 2017). While individual contextual information might be an appropriate approach for many research purposes – such as identifying gender discrimination in computer sciences (Buolamwini & Gebru, 2018; Sasha Costanza-Chock, 2018) – this study has shown that formalized, de-contextual approaches that systematize managerial actions are important for providing a structured framing for making complex decisions aimed at protecting the very causes for which critical data studies are advocating, such as race and gender equality. The information architecture derived from human rights due diligence helps to ensure a rights-based approach, even under high political encumbrance and intense time pressure. In a way, a sensemaking approach through elite interviewing can serve as a novel approach to study socio-political constructs in the data economy. By unpacking the complexities in decision-making processes within tech companies, this method can deliver important insights (e.g. how companies aim at making their products and services rights-respecting for users across different geographies), and how they respond and adapt to local contexts and needs, and by that counter the criticism of “data colonialism” (Couldry & Mejias, 2019; Kotliar, 2020).

To a certain extent, calling for information architecture that supports a systematic, formal approach for ensuring basic respect for human dignity could complement current data justice literature in meaningful ways. The complementarity between formality and contextuality lies at the very heart of understanding the social impacts of technology. For example, contextual studies can shine light on emerging issues that would need to be incorporated in the systematized management process on human rights, while the human rights due diligence architecture provides the analytical grid for communicating, reporting and mitigating adverse human rights impacts within the company. As studies with a contextual focus discover emerging human rights issues, such findings can be distilled through the established B&HR avenues, potentially making managerial re-configurations necessary. Yet the B&HR architecture enables a fast, more coordinated, response in big technology companies who might be otherwise very slow at organizational change or making space for the needs highlighted in critical data studies. For critical data studies scholars, this research suggests that theories about black box algorithms may need to be revised in light of management’s strong stake in determining the design, roll-out and implementation of data usage and governance, and the ability to abort certain data sharing in light of political tensions. The complementarity of a B&HR approach and critical data studies is apparent: in order to assess the legality, necessity and proportionality of an action as required by Internal Human Rights Law and further

substantiated by the Necessary & Proportionate principles (EFF, 2014), decision-makers need contextual information to make an assessment. An example of such complementarity would be a human rights-based approach to data-driven workplace management that would require close alignment with a systematic human rights due diligence approach, e.g. the development of a methodology to prevent racial discrimination in algorithmic models (Hanna, Denton, Smart, & Smith-Loud, 2020).

At the same time, the findings point also to areas that would benefit from further research, both to substantiate initial suppositions and to connect the findings to business and human rights scholarship, critical data studies and sensemaking literature. For business and human rights scholars, while this work shows that decisions taken by companies on technology have enormous human rights implications that may require well-designed and thorough decision-making criteria for crisis situations, a strong organizational backbone can cushion against the avalanche of human rights risks associated with data requests. The close communication structures that companies create to ensure sound alignment between the headquarter and subsidiaries contrasts with earlier B&HR sensemaking literature that showed that companies prefer an overall vague CSR framing, with the more precise B&HR as a subcomponent of that (Obara, 2017, p. 271). Given that empirical studies – and in particular sensemaking studies – in the B&HR literature are so far sparse, further research could investigate if and how sensemaking in crisis situations uses a human rights framework in other business sectors, and how sensemaking dimensions interrelate. Further research could also explore whether sensemaking in crisis leads to closer communications between headquarter and subsidiary, in contrast to earlier claims by companies that they cannot sufficiently control their subsidiaries' actions for respecting human rights down to the local level (Kobrin, 2009; Matheson, 2008; Ruggie, 2014; Skinner, 2015). Such research should also relate to the question of whether it is the digital nature of government data disclosure requests that enables this close alliance between headquarter and subsidiary when responding to government pressure. This constellation might change when the subject matter is not “digital” but relates to “physical” matters and/or assets, – such as withholding or confiscating corporate commodities by the local government – and when there is sparse information about the situation on the ground.

Relatedly, the findings allow for further theorizing about the tension between the state duty to protect human rights stemming from the use of digital technology, and the corporate responsibility to respect human rights. These issues around normative conflicts and the tension between pillar I and pillar II of the UNGPs have been clearly reflected in the findings, as interviewees repeatedly stressed that they have general policies and practices to deal with unconventional data disclosure requests; yet the current fragmented framework and underlying normative conflicts make a case-by-case analysis necessary. In contrast, access to remedy (pillar III of the UNGPs) has hardly been addressed in the interview material, neither in a judicial, nor non-judicial, sense and would require further explorations in future research. Eventually, the friction between the companies' role in data collection efforts and enabling data access to governments in the first place renders access to remedy more or less obsolete due to the almost non-existent possibility of informing a data subject when their data has

been requested. In the second place, by accessing sensitive data in highly politicized settings, fragile states or legal grey areas, the government is not acting in a rights-respecting manner and is therefore unlikely to facilitate access to remedy, as it would be its duty. Here, the different options for calibrating between solutions relying on local accountability mechanisms and/or the group level as a protective function emerged in the sensemaking as a response to normative frictions across jurisdictions. This case-by-case analysis departs from a multi-centric assessment to see how a request could potentially negatively impact rights holders if their data is shared with a government with a debatable human rights record. Further research might usefully investigate the relationship between the opacity of data disclosure requests and the public communications on human rights by companies, in order to hold governments accountable and have them exert a human rights-based approach when requesting user data from companies. The duty of government to act on a human rights-based approach needs further investigation, especially in light of increasing security narratives. On the flipside, further research might also investigate whether companies are systematically using a human rights framing to achieve their own interests when responding to data disclosure requests, and aiming to blame misconduct on the government. For example, it could be investigated whether the legal limitations actually lead to a mismatch between action happening inside the company and the companies' external communications around this issue (see chapter VI. 3.), or whether (also) the companies rely heavily on obfuscation to achieve their own ends, e.g. continue with relentless data maximization efforts.

From a critical data studies perspective, the role played by data maximization as a core feature of platforms' business models was here underexplored due to its absence in the empirical data from the interviews. The role of data maximization was not a subject of reflection for the interview participants, and brought up only by a few minority voices in civil society and some telecommunications representatives to demonstrate the differences between telecommunications and platform business models. As data maximization produces the very vastness of data that ultimately makes individuals vulnerable (Eubanks, 2018; O'Neil, 2017), it is interesting that the interviewees appear to take data maximization for granted, as a sort of "necessary evil" and/or did not see it as strongly related to the subject of data disclosure requests. This is quite remarkable, especially in light of the way some interviewees outlined a minimization response to government. Companies are vulnerable to government requests because they hold such complete data, but minimizing the amount of data collected in the first place is not conceived of as an option. Of considerable importance with regard to the human rights conduct of the technology sector is also the question of de-facto ownership of digital infrastructure and to what extent the state holds sufficient leverage to be able to effectively determine governance structures. This is also an aspect that would allow for further research, e.g. on the interdependency between corporate infrastructure and government interception in the form of obligatory interfaces for the government provided by internet service providers (ETSI, 2006), as big social media platforms also ultimately rely on the internet service providers' services for their data routes.

Rights-respecting management practices can address the phenomena of human rights risks and mitigate negative impacts arising from the paradoxical relationship between companies and the state with regard to data sharing, all while the networked effects on normative tensions in internet governance persist. The root causes lie deep within the conflicting normative assumptions across jurisdictions as to what privacy actually constitutes, and under which circumstances it is socially acceptable to invade an individual's private life. The quantification of the social order extends across a plethora of black box boxes in society (Pasquale, 2015). This has the potential to fundamentally change how we perceive our lifeworlds. The data emerging from quantifying the social and the information that data holds therefore need to be safeguarded wisely. The need for safeguards in data management and oversight mechanisms has been powerfully demonstrated by global health management efforts around the COVID-19 pandemic, which put a spotlight on intrusive data gathering and related privacy effects, as well as the potential benefits of using human data in correct ways to evaluate and partly anticipate the behaviour of population groups (B-Tech, 2020).

In the years to come, quantification will hopefully shine light into the darkness around human behaviour in conflicts, as abusive behaviour by actors increasingly leaves data traces. One could imagine that data logs could become an important feature in post-conflict processes by allowing human rights abusers, such as natural persons, companies, and also state actors, to be held account (Pietropaoli, 2020). The attempts to analyse data from Facebook (Ochab, 2020; Smith, 2020) in relation to conflict retracing and resolution show that human behaviour nowadays is quantified, even in conflicts, and can therefore be a factor that enables and upholds, as well as infringes upon, human rights. Digital evidence then becomes a powerful tool for holding perpetrators of human rights violations to account, in some instances with higher levels of information granularity than paper-based documentation.

To conclude on a more uplifting note with Habermas (1970, 1995), the research has shown that a sensemaking approach which relies on a human rights framing of data disclosure requests helps in a company's practice by critically revisiting the paradigm of technological control. Human rights have proven to provide essential protection for the magic beauty of the social lifeworld with its free, open, and communicative character, upon which rests the deliberative force of democracy.

References

- AccessNow. (2018). Human rights in the age of artificial intelligence. . Retrieved from <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>
- Addo, M. K. (2014). The reality of the United Nations guiding principles on business and human rights. *Human Rights Law Review*, 14(1), 133-147.
- Alimardani, M., & Milan, S. (2018). The internet as a global/local site of contestation: The case of Iran. In *Global cultures of contestation* (pp. 171-192). London: Palgrave Macmillan.
- Alston, P. (2006). *Non State Actors and Human Rights*. Oxford: Oxford University Press.
- Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New media & society*, 20(3), 973-989.
- Arun, C. (2020). AI and the Global South. In M. Dubber, F. Pasquale, & S. Das (Eds.), *The Oxford Handbook of Ethics of AI*. Oxford: Oxford University Press.
- Awori, S., Anumo, F., Montes, D. C., & Hughes, L. (2018). A feminist approach to the binding instrument on transnational corporations and other business enterprises. *Business and Human Rights Journal*, 3(2), 285-290.
- B-Tech. (2020). UN Human Rights B-Tech's IGF panel. "Upholding Rights in the State-Business Nexus: C19 and beyond" [Press release]. Retrieved from https://www.ohchr.org/Documents/Issues/Business/B-Tech/write-up_IGF_panel.pdf
- Ball, K. (2010). Workplace surveillance: An overview. *Labor History*, 51(1), 87-106.
- Baumann-Pauly, D., & Nolan, J. (2016). *Business and human rights: From principles to practice*. London/New York: Routledge.
- Benjamin, R. (2019). *Race after technology: Abolitionist Tools for the New Jim Code*. Boston: Polity.
- Bernal, P. (2016). Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy*, 1(2), 243-264.
- Bernaz, N. (2013). Enhancing corporate accountability for human rights violations: is extraterritoriality the magic potion? *Journal of Business Ethics*, 117(3), 493-511.
- Berry, J. M. (2002). Validity and reliability issues in elite interviewing. *PS: Political Science and Politics*, 35(4), 679-682.
- Blumberg, A. J., & Eckersley, P. (2009). On locational privacy, and how to avoid losing it forever. Retrieved from <https://www.eff.org/files/eff-locational-privacy.pdf>
- Boghosian, H. (2012). The Business of Surveillance. *Human Rights*, 39, 2.
- boyd, d., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, communication & society*, 15(5), 662-679.
- Buolamwini, J. (2018). When AI misclassified her face, she started a movement for accountability. Retrieved from <https://www.technologyreview.com/lists/innovators-under-35/2018/pioneer/joy-buolamwini/>
- Buolamwini, J. (2018, June 21st, 2018). When the Robot Doesn't See Dark Skin. The New York Times Retrieved from <https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html>
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Paper presented at the Conference on Fairness, Accountability and Transparency, Proceedings of Machine Learning Research 81:1–15.
- Bygnes, S. (2008). Interviewing people-oriented elites. Paper presented at the Eurosphere Online Working Paper Series, Bergen: University of Bergen.
- Cardozo, N., Cohn, C., Higgins, P., Opsahl, K., & Reitman, R. (2014). Who has your back? Protecting your data from government requests. Retrieved from <https://www.eff.org/de/node/81897>

- Case C-362/14, Maximilian Schrems v Data Protection Commissioner (Court of Justice of the European Union 2015).
- Case C-311/18 (Court of Justice of the European Union 2020).
- Castells, M. (2012). *Networks of outrage and hope: Social movements in the Internet age*. Chichester: John Wiley & Sons.
- Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the 'good society': the US, EU, and UK approach. *Science and engineering ethics*, 24(2), 505-528.
- Chandler, G. (2003). The evolution of the business and human rights debate. In R. Sullivan (Ed.), *Business and Human Rights* (pp. 22-32). Sheffield: Greenleaf Publishing.
- Clapham, A. (2006). *Human rights obligations of non-state actors*. Oxford: Oxford University Press.
- Cohen, J. E. (2012). What privacy is for. *Harvard Law Review*, 126, 1904-1933.
- Cohen, J. E. (2016). The surveillance-innovation complex: The irony of the participatory turn. In D. Barney, G. Coleman, C. Ross, J. Sterne, & T. Tembeck (Eds.), *The Participatory Condition* Minnesota University of Minnesota Press
- Collier, P. (2008). *The Bottom Billion - Why the poorest countries are failing and what can be done about it*. Oxford: Oxford University Press.
- Collier, P., Elliott, V. L., Hegre, H., Hoeffler, A., Reynal-Querol, M., & Sambanis, N. (2003). *Breaking the conflict trap: Civil war and development policy*. Retrieved from Washington D.C.: <https://openknowledge.worldbank.org/handle/10986/13938>
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). , (2016).
- Commission, E. (2019). *E-evidence - cross-border access to electronic evidence: Improving cross-border access to electronic evidence*. Retrieved from https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en
- Confessore, N. (2018, April 4th, 2018). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times* Retrieved from <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>
- Congress, U. S. (2018). *Clarifying Lawful Overseas Use of Data Act or the CLOUD Act*. Retrieved from <https://www.congress.gov/bill/115th-congress/house-bill/4943>
- Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No.005, Council of Europe (1950 September 3rd, 1953).
- Costanza-Chock, S. (2018). *Design Justice: towards an intersectional feminist framework for design theory and practice*. Proceedings of the Design Research Society. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3189696
- Costanza-Chock, S., Wagoner, M., Taye, B., Rivas, C., Schweidler, C., & Bullen, G. (2018). *#More than Code. Practitioners reimagine the landscape of technology for justice and equity*. Retrieved from https://morethancode.cc/T4SJ_Exec_Summ_final_web.pdf
- Couldry, N., & Mejias, U. A. (2019). Data colonialism: rethinking big data's relation to the contemporary subject. *Television & New Media*, 20(4), 336-349.
- Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review*, 55(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. *Foreign Affairs* 92, 27-40.
- De Felice, D., & Graf, A. (2015). The Potential of National Action Plans to Implement Human Rights Norms: An Early Assessment with Respect to the UN Guiding Principles on Business and Human Rights. *Journal of Human Rights Practice*, 7(1), 40-71.

- De Schutter, O., Ramasastry, A., Taylor, M. B., & Thompson, R. C. (2012). Human Rights Due Diligence: The Role of States. Retrieved from <https://corporatejustice.org/hrdd-role-of-states-3-dec-2012.pdf>
- DeBrusk, C. (2018). The Risk of Machine-Learning Bias (and How to Prevent It). MIT Sloan Management Review. Retrieved from <https://sloanreview.mit.edu/article/the-risk-of-machine-learning-bias-and-how-to-prevent-it/>
- Deibert, R. (2008). The geopolitics of internet control: Censorship, sovereignty, and cyberspace. In Routledge Handbook of Internet Politics (pp. 339-352). New York/London: Routledge.
- Deibert, R. (2015a). Authoritarianism goes global: Cyberspace under siege. *Journal of Democracy*, 26(3), 64-78.
- Deibert, R. (2015b). The geopolitics of cyberspace after Snowden. *Current History*, 114(768), 9-15.
- Deibert, R. (2019). The Road to Digital Unfreedom: Three Painful Truths About Social Media. *Journal of Democracy*, 30(1), 25-39.
- Delaney, K. J. (2007). Methodological dilemmas and opportunities in interviewing organizational elites. *Sociology Compass*, 1(1), 208-221.
- Deva, S. (2003). Human rights violations by multinational corporations and international law: where from here. *Conneticut Journal of International Law*, 19, 1-57.
- Deva, S. (2016). Bhopal: The saga continues 31 years on. In D. Baumann-Pauly & J. Nolan (Eds.), *Business and human rights: From principles to practice* (pp. 22-26). New York/London: Routledge.
- Deva, S., & Bilchitz, D. (2013). *Human rights obligations of business: beyond the corporate responsibility to respect?* Cambridge: Cambridge University Press.
- Deva, S., Ramasastry, A., Santoro, M., & Wettstein, F. (2019). Editorial: Business and Human Rights Scholarship: Past Trends and Future Directions. *Business & Human Rights Journal* 4(2), 201-212.
- Diamond, L. (2010). Liberation technology. *Journal of Democracy*, 21(3), 69-83.
- Diamond, L. (2015). Liberation technology. In L. Diamond & M. F. Plattner (Eds.), *Liberation Technology - Social Media and the Struggle for Democracy* (pp. 3-17). Baltimore: The John Hopkins University Press
- Dingwerth, K., & Pattberg, P. (2006). Global governance as a perspective on world politics. *Global Governance*, 12(2), 185-204.
- Ebert, I. (2019). The Tech Company Dilemma. *Ethical Managerial Practice in Dealing with Government Data Requests*. *zfwu Zeitschrift für Wirtschafts-und Unternehmensethik*, 20(2), 264-275.
- Ebert, I., Busch, T., & Wettstein, I. F. (2020). Business and Human Rights in the Data Economy. Retrieved from German Institute for Human Rights: https://www.institut-fuer-menschenrechte.de/fileadmin/user_upload/Publikationen/ANALYSE/Analysis_Business_and_Human_Rights_in_the_Data_Economy.pdf
- EFF. (2014). Necessary & Proportionate Principles Retrieved from <https://necessaryandproportionate.org/principles/>
- EFF. (2020). About. Retrieved from <https://www.eff.org/about>
- Elsawah, M., Howard, P. N., & Narayanan, V. (2019). Iranian digital Interference in the Arab World. Data Memo. Project on Computational Propaganda, Oxford, United Kingdom, 1850-1867. Retrieved from <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/04/Iran-Memo.pdf>
- Engelhardt, T. (2019). Who pays? On artificial agents, human rights and tort law. In B. Wagner, M. C. Kettemann, & K. Vieth (Eds.), *Research Handbook on Human Rights and Digital Technology*. Cheltenham, UK/Northampton, US: Edward Elgar Publishing.
- ETSI. (2006). Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture. Retrieved from https://www.etsi.org/deliver/etsi_tr/101900_101999/101943/02.02.01_60/tr_101943v020201p.pdf

- Eubanks, V. (2018). *Automating Inequality: How high-tech tools profile, police and punish the poor*. New York: St. Martin's Press.
- Europe, C. o. (2001). *The Budapest Convention 24/7 Points of Contact Network*. Retrieved from <https://rm.coe.int/1680081561>
- Facebook. (2020). *Law Enforcement Guidelines*. Retrieved from <https://www.facebook.com/safety/groups/law/guidelines>
- Fasterling, B. (2017). Human rights due diligence as risk management: Social risk versus human rights risk. *Business and Human Rights Journal*, 2(2), 225-247.
- Feng, H. (2007). New Developments in Mutual Legal Assistance in Criminal Matters. *Contemporary Law Review*(6), 3.
- Fiss, P. C., & Zajac, E. J. (2006). The symbolic management of strategic change: Sensegiving via framing and decoupling. *Academy of management journal*, 49(6), 1173-1193.
- Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2020). Authority conflicts in internet governance: Liberals vs. sovereigntists? *Global Constitutionalism*, 9(2), 364-386.
- Flyverbom, M., Deibert, R., & Matten, D. (2019). The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business. *Business & Society*, 58(1), 3-19. doi:10.1177/0007650317727540
- Frank, A. G. (1966). *The development of underdevelopment*. Boston: New England Free Press.
- Frei, L., & Trechsel, S. (1990). Origins and Applications of the United States-Switzerland Treaty on Mutual Assistance in Criminal Matters. *Harvard International Law Journal*, 31, 77.
- Freyburg, T., & Garbe, L. (2018). Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa. *International Journal of Communication*, 12, 3896-3916.
- Gasser, U., & Almeida, V. A. (2017). A layered model for AI governance. *IEEE Internet Computing*, 21(6), 58-62.
- Gillespie, T. (2010). The politics of 'platforms'. *New media & society*, 12(3), 347-364.
- Gillespie, T. (2014). The relevance of algorithms. *Media technologies: Essays on communication, materiality, and society*, 167(2014), 167.
- Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. New Haven: Yale University Press.
- Gioia, D., & Chittipeddi, K. (1991). Sensemaking and sensegiving in strategic change initiation. *Strategic management journal*, 12(6), 433-448.
- Gioia, D., Corley, K., & Hamilton, A. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, 16(1), 15-31. doi:10.1177/1094428112452151
- Gioia, D., Thomas, J., Clark, S., & Chittipeddi, K. (1994). Symbolism and strategic change in academia: The dynamics of sensemaking and influence. *Organization science*, 5(3), 363-383.
- Glasius, M., & Michaelsen, M. (2018). Authoritarian Practices in the Digital Age| Illiberal and Authoritarian Practices in the Digital Sphere—Prologue. *International Journal of Communication*, 12, 3788-3794.
- GNI. (2017). *GNI Principles on Freedom of Expression and Privacy*. Retrieved from <https://globalnetworkinitiative.org/wp-content/uploads/2018/04/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf>
- GNI (Producer). (2020a). *The GNI Principles at Work*. Public Report on the Third Cycle of Independent Assessments of GNI Company Members. Retrieved from <https://globalnetworkinitiative.org/wp-content/uploads/2020/04/2018-2019-PAR.pdf>
- GNI. (2020b). *Members*. Retrieved from <https://globalnetworkinitiative.org/#home-menu>
- Goethals, S. (2019). Exploring Migrant Employees' Rights-Talk in the British Hospitality Sector. *Business and Human Rights Journal*, 4(2), 287-315.
- Google. (2020). *Transparency Report*. Retrieved from <https://transparencyreport.google.com/?hl=en>

- Götzmann, N. (2017). Human rights impact assessment of business activities: Key criteria for establishing a meaningful practice. *Business and Human Rights Journal*, 2(1), 87-108.
- Götzmann, N. (2019). *Handbook on Human Rights Impact Assessment*. Cheltenham, UK
Northampton, MA: Edward Elgar.
- Government, U. (2016). Investigatory Powers Act Retrieved from <https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted>
- Grabenwarter, C. (2014). *European convention on human rights: commentary*. Munich: CH Beck.
- Graham, M. (2019). There are no rights 'in' cyberspace. In *Research Handbook on Human Rights and Digital Technology*. Cheltenham, UK/Northampton, MA: Edward Elgar Publishing.
- Graham, M., Hjorth, I., & Lehdonvirta, V. (2017). Digital labour and development: impacts of global digital labour platforms and the gig economy on worker livelihoods. *Transfer: European Review of Labour and Research*, 23(2), 135-162.
- Gray, D., & Henderson, S. E. (2017). *The Cambridge Handbook of Surveillance Law*. Cambridge, UK: Cambridge University Press.
- Greenwald, G. (2015). *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Toronto: McClelland & Stewart.
- Greenwald, G., MacAskill, E., & Poitras, L. (2013). Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*, p. 2.
- Habermas, J. (1970). *Toward a rational society: Student protest, science, and politics*. Boston: Beacon Press.
- Habermas, J. (1981). *Theorie des kommunikativen Handelns* (Vol. 2). Frankfurt: Suhrkamp Frankfurt.
- Habermas, J. (1995). *Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats*. Frankfurt a.M.: Suhrkamp.
- Hanna, A., Denton, E., Smart, A., & Smith-Loud, J. (2020). Towards a critical race methodology in algorithmic fairness. Paper presented at the Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency.
- Hern, A. (2020). Facebook and WhatsApp pause Hong Kong user data requests. *The Guardian* Retrieved from <https://www.theguardian.com/world/2020/jul/06/facebook-whatsapp-pause-hong-kong-user-data-requests>
- Howard, P. N. (2015). *Pax Technica: How the Internet of things may set us free or lock us up*. New Haven: Yale University Press.
- Howard, P. N., & Hussain, M. M. (2011). The upheavals in Egypt and Tunisia: The role of digital media. *Journal of Democracy*, 22(3), 35-48.
- Israel, B. R. (2009). Make Money without Doing Evil-Caught between Authoritarian Regulations in Emerging Markets and a Global Law of Human Rights, *US ICTs Face a Twofold Quandary*. *Berkeley Technology Law Journal*, 24, 617.
- Jiang, M. (2016). Chinese internet business and human rights. *Business and Human Rights Journal*, 1(1), 139-144.
- Jørgensen, R. F. (2017). What Platforms Mean When They Talk About Human Rights. *Policy & Internet*, 9(3), 280-296.
- Jørgensen, R. F. (2018). Framing human rights: exploring storytelling within internet companies. *Information, communication & society*, 21(3), 340-355.
- Jørgensen, R. F. (2019). *Human rights in the age of platforms*: The MIT Press.
- Kellogg, K. C., Valentine, M. A., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. *Academy of Management Annals*, 14(1), 366-410.
- Keohane, R. O., & Nye, J. S. (1977). *Power and interdependence*. Boston: Little, Brown & Co.
- Kinley, D., Nolan, J., & Zerial, N. (2007). The politics of corporate social responsibility: Reflections on the United Nations Human Rights Norms for Corporations. *Company and Securities Law Journal*, 25(1), 30-42.

- Kobrin, S. J. (2009). Private political authority and public responsibility: Transnational politics, transnational firms, and human rights. *Business Ethics Quarterly*, 349-374.
- Koehler, J. O. (1999). *STASI: The untold story of the East German secret police*. Boulder, US/Oxford, UK: Westview Press.
- Kotliar, D. (2020). Data orientalism: on the algorithmic construction of the non-Western other. *Theory and Society*. Retrieved from <https://link.springer.com/article/10.1007/s11186-020-09404-2>
- Krishnamurthy, V. (2019). Are Internet Protocols the New Human Rights Protocols? Understanding 'RFC 8280—Research into Human Rights Protocol Considerations'. *Business and Human Rights Journal*, 4(1), 163-169.
- Labowitz, S. P., Michael. (2016). Why We're Leaving the Global Network Initiative. Retrieved from <https://bhr.stern.nyu.edu/blogs/why-were-leaving-the-gni>
- Latonero, M. (2018). Governing artificial intelligence: Upholding human rights & dignity. Retrieved from https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf
- Latonero, M., & Kift, P. (2018). On digital passages and borders: Refugees and the new infrastructure for movement and control. *Social Media+ Society*, 4(1), 1-11.
- Latour, B. (2005). *Reassembling the social: an introduction to Actor-Network Theory*. Oxford: Oxford University Press.
- Lindlof, T. R., & Taylor, B. C. (2017). *Qualitative communication research methods*. Thousand Oaks, California: Sage publications.
- Livingston, S., & Risse, M. (2019). The future impact of artificial intelligence on humans and human rights. *Ethics & international affairs*, 33(2), 141-158.
- Lynch, M. (2011). After Egypt: The limits and promise of online challenges to the authoritarian Arab state. *Perspectives on politics*, 9(2), 301-310.
- MacKinnon, R. (2007). Shi Tao, Yahoo!, and the lessons for corporate social responsibility. Retrieved from <https://cyberdialogue.ca/wp-content/uploads/2011/03/Rebecca-MacKinnon-Shi-Tao-Yahoo-and-the-Lessons-for-CSR.pdf>
- MacKinnon, R. (2011). Liberation Technology: China's "Networked Authoritarianism". *Journal of Democracy*, 22(2), 32-46.
- MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for Internet freedom*. New York Basic Books.
- MacKinnon, R., Hickok, E., Bar, A., & Lim, H.-i. (2015). *Fostering freedom online: The role of internet intermediaries*. Paris: UNESCO Publishing.
- Macklin, A., & Simons, P. (2014). *Extractive Industries, Human Rights, and the Home State Advantage*. London/New York: Routledge.
- Maclay, C. M. (2010). Protecting Privacy and Expression Online: Can the Global Network Initiative Embrace the Character of the Net? In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access Controlled, The Shaping Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press.
- Maitlis, S. (2005). The social processes of organizational sensemaking. *Academy of management journal*, 48(1), 21-49.
- Maitlis, S., & Christianson, M. (2014). Sensemaking in organizations: Taking stock and moving forward. *Academy of Management Annals*, 8(1), 57-125.
- Maitlis, S., & Lawrence, T. B. (2007). Triggers and enablers of sensegiving in organizations. *Academy of management journal*, 50(1), 57-84.
- Maitlis, S., & Sonenshein, S. (2010). Sensemaking in crisis and change: Inspiration and insights from Weick (1988). *Journal of management studies*, 47(3), 551-580.
- Maréchal, N. (2015). Ranking Digital Rights: Human Rights, the Internet and the Fifth Estate. *International Journal of Communication*, 9, 10.
- Martin-Ortega, O. (2008). Business and human rights in conflict. *Ethics & international affairs*, 22(3), 273-283.

- Matheson, J. H. (2008). The modern law of corporate groups: An empirical study of piercing the corporate veil in the parent-subsidary context. *North Carolina Law Review*, 87, 1091.
- Mau, S. (2019). *The metric society: On the quantification of the social*. Cambridge, MA: Polity.
- Mayer-Schönberger, V., & Ramge, T. (2018). *Reinventing capitalism in the age of big data*. New York: Basic Books.
- Mazzucato, M. (2011). The entrepreneurial state. *Soundings*, 49(49), 131-142.
- McCorquodale, R., Lise, S., Neely, S., & Brooks, R. (2017). Human Rights Due Diligence in Law and Practice: Good Practices and Challenges for Business Enterprises §. *Business and Human Rights Journal*, 2(2), 195-224.
- Mennicken, A., & Espeland, W. N. (2019). What's new with numbers? Sociological approaches to the study of quantification. *Annual Review of Sociology*, 45, 223-245.
- Mhlambi, S. (2020). From Rationality to Relationality: Ubuntu as an Ethical and Human Rights Framework for Artificial Intelligence Governance. Retrieved from <https://carrcenter.hks.harvard.edu/publications/rationality-relationality-ubuntu-ethical-and-human-rights-framework-artificial>
- Michalowski, S. (2014). *Corporate accountability in the context of transitional justice*. New York: Routledge.
- Milan, S., & Treré, E. (2019). Big data from the South (s): Beyond data universalism. *Television & New Media*, 20(4), 319-335.
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Thousand Oaks, California: Sage.
- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1-21.
- Moore, M., & Tambini, D. (2018). *Digital dominance: the power of Google, Amazon, Facebook, and Apple*. Oxford: Oxford University Press.
- Moss, D. M. (2018). The ties that bind: Internet communication technologies, networked authoritarianism, and 'voice' in the Syrian diaspora. *Globalizations*, 15(2), 265-282.
- Neff, G., Jordan, T., McVeigh-Schultz, J., & Gillespie, T. (2012). Affordances, Technical Agency, and the Politics of Technologies of Cultural Production. *Journal of Broadcasting & Electronic Media*, 56(2), 299-313. doi:10.1080/08838151.2012.678520
- Neff, G., & Nafus, D. (2016). *Self-tracking*. Cambridge, MA: MIT Press.
- Neff, G., Tanweer, A., Fiore-Gartland, B., & Osburn, L. (2017). Critique and contribute: A practice-based framework for improving critical data studies and data science. *Big data*, 5(2), 85-97.
- Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York: New York University Press.
- Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. Paper presented at the Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems.
- NOYB. (2020). CJEU invalidates "Privacy Shield" in US Surveillance case. SCCs cannot be used by Facebook and similar companies. [Press release]. Retrieved from <https://noyb.eu/en/cjeu>
- O'Neil, C. (2017). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York: Broadway Books.
- O'Brien, C. M., Mehra, A., Blackwell, S., & Poulsen-Hansen, C. B. (2016). National action plans: Current status and future prospects for a new business and human rights governance tool. *Business and Human Rights Journal*, 1(1), 117-126.
- O'Neil, C. (2017). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York: Broadway Books.
- Obara, L. J. (2017). 'What Does This Mean?': How UK Companies Make Sense of Human Rights. *Business and Human Rights Journal*, 2(2), 249-273.

- Obara, L. J., & Peattie, K. (2018). Bridging the great divide? Making sense of the human rights-CSR relationship in UK multinational companies. *Journal of World Business*, 53(6), 781-793.
- Ochab, E. (2020). Could Facebook Help To Establish The Burmese Government's Intent To Commit Genocide Against The Rohingya Muslims? *Forbes*. Retrieved from <https://www.forbes.com/sites/ewelinaochab/2020/07/06/could-facebook-help-to-establish-the-burmese-governments-intent-to-commit-genocide-against-the-rohingya-muslims/#29b20e8a195b>
- OHCHR. (2015). Special Rapporteur on the Right to Privacy Retrieved from <https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx>
- OHCHR. (2019). UN Human Rights Business and Human Rights in Technology Project (B-Tech). Applying the UN Guiding Principles on Business and Human Rights to digital technologies. Retrieved from [https://www.ohchr.org/Documents/Issues/Business/B-Tech/B %20Tech Project revised scoping final.pdf](https://www.ohchr.org/Documents/Issues/Business/B-Tech/B%20Tech%20Project%20revised%20scoping%20final.pdf)
- OHCHR. (2020). The B-Tech project. Retrieved from <https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx>
- Parsons, C. (2019). The (in) effectiveness of voluntarily produced transparency reports. *Business & Society*, 58(1), 103-131.
- Pasquale, F. (2015). *The black box society*. Cambridge, MA: Harvard University Press.
- Pauwelyn, J., Wessel, R. A., & Wouters, J. (2014). When structures become shackles: stagnation and dynamics in international lawmaking. *European Journal of International Law*, 25(3), 733-763.
- Peet, R., & Hartwick, E. (2015). *Theories of development: Contentions, arguments, alternatives*. New York: Guilford Publications.
- Perez, C. C. (2019). *Invisible Women: Exposing Data Bias in a World Designed for Men*. New York Vintage Publishing
- Pietropaoli, I. (2020). *Business, Human Rights and Transitional Justice*. New York: Routledge.
- Porter, T. M. (1986). *The rise of statistical thinking, 1820-1900*. Princeton: Princeton University Press.
- Porter, T. M. (1996). *Trust in numbers: The pursuit of objectivity in science and public life*. Princeton: Princeton University Press.
- Prassl, J. (2018). *Humans as a service: The promise and perils of work in the gig economy*. Oxford: Oxford University Press.
- Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. *Journal of Democracy*, 30(1), 53-67.
- Rahman, A. (2016). Improving the transparency of government requests for user data from ICT companies. Massachusetts Institute of Technology, Massachusetts Institute of Technology. Retrieved from <https://dspace.mit.edu/handle/1721.1/104826>
- Ramasastri, A. (2015). Corporate social responsibility versus business and human rights: Bridging the gap between responsibility and accountability. *Journal of Human Rights*, 14(2), 237-259.
- Raso, F. A., Hilligos, H., Krishnamurthy, V., Bavitz, C., & Kim, L. (2018). Artificial Intelligence & Human Rights: Opportunities & Risks. In B. K. C. R. P. n. 2018-6. (Ed.). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3259344
- RDR. (2019). Executive Summary 2019 index. Retrieved from <https://rankingdigitalrights.org/index2019/report/executive-summary/>
- RDR. (2020a). Methodology. Retrieved from <https://rankingdigitalrights.org/index2019/report/index-methodology/>
- RDR. (2020b). Ranking Digital Rights. Retrieved from <https://rankingdigitalrights.org/>
- Reventlow, N. J. (2019). Digital rights are *all* human rights, not just civil and political. Retrieved from <https://medium.com/berkman-klein-center/digital-rights-are-all-human-rights-not-just-civil-and-political-daf1f1713f7a>
- Ricaurte, P. (2019). Data epistemologies, the coloniality of power, and resistance. *Television & New Media*, 20(4), 350-365.

- Richards, D. (1996). Elite interviewing: Approaches and pitfalls. *Politics*, 16(3), 199-204.
- Richardson, R., Schultz, J., & Crawford, K. (2019). Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York University Law Review Online*, 94(15).
- Rigot, A. (2018). Apps and traps: why dating apps must do more to protect LGBTQ communities. Retrieved from <https://www.openglobalrights.org/apps-and-traps-why-dating-apps-must-do-more-to-protect-LGBTQ-communities/>
- Risse, M. (2019). Human rights and artificial intelligence: An urgently needed agenda. *Human Rights Quarterly*, 41(1), 1-16.
- Ruggie, J. G. (2007). Business and human rights: the evolving international agenda. *American Journal of International Law*, 101(4), 819-840.
- Ruggie, J. G. (2013). *Just business: Multinational corporations and human rights* New York/London: WW Norton & Company.
- Ruggie, J. G. (2014). Global governance and "new governance theory": Lessons from business and human rights. *Global Governance: A Review of Multilateralism and International Organizations*, 20(1), 5-17.
- Rydzak, J. A. (2018). *A Total Eclipse of the Net: The Dynamics of Network Shutdowns and Collective Action Responses*. University of Arizona.
- Sachs, J. D. (2006). *The end of poverty: Economic possibilities for our time*. New York: Penguin.
- Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, 6(1), 1-12.
- Samway, M. (2016). The Global Network Initiative: How can companies in the information and communications technology industry respect human rights. In D. Baumann-Pauly & J. Nolan (Eds.), *Business and human rights: From principles to practice* (pp. 136-146). New York: Routledge.
- Samway, M., & Ryan, W. (2014). The Internet, Human Rights, and the Private Sector. *Georgetown Journal of International Affairs*, 25-32.
- Santoro, M. A. (2015). Business and human rights in historical perspective. *Journal of Human Rights*, 14(2), 155-161.
- 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. *Journal of management studies*, 48(4), 899-931.
- Schrempf-Stirling, J., & Van Buren, H. J. (2017). Bringing human rights together with management studies: Themes, opportunities, and challenges. Paper presented at the Academy of Management Proceedings.
- Sen, A. (1999). *Development as freedom*. Oxford: Oxford University Press.
- Skinner, G. (2015). Rethinking limited liability of parent corporations for foreign subsidiaries' violations of international human rights law. *Washington and Lee Law Review*, 72, 1769-1864.
- Sloane, M. (2018). Making artificial intelligence socially just: Why the current focus on ethics is not enough. Retrieved from <https://blogs.lse.ac.uk/politicsandpolicy/artificial-intelligence-and-society-ethics/>
- Smith, M. (2020). Facebook Wanted to Be a Force for Good in Myanmar. Now It Is Rejecting a Request to Help With a Genocide Investigation. *Time*. Retrieved from <https://time.com/5880118/myanmar-rohingya-genocide-facebook-gambia/>
- Snow, D. A. (1980). The disengagement process: A neglected problem in participant observation research. *Qualitative sociology*, 3(2), 100-122.
- Soghoian, C. (2011). An end to privacy theater: Exposing and discouraging corporate disclosure of user data to the government. *Minnesota Journal of Law, Science & Technology*, 12, 191-237.
- Solon, O. (2016, 12 December). 2016: The year Facebook became the bad guy. *TheGuardian*. Retrieved from <https://www.theguardian.com/technology/2016/dec/12/facebook-2016-problems-fake-news-censorship>

- Srnicek, N. (2017). Platform capitalism. Cambridge: Polity.
- Strauss, A. L. (1987). Qualitative analysis for social scientists. Cambridge, UK: Cambridge University Press.
- Taylor, L., & Broeders, D. (2015). In the name of Development: Power, profit and the datafication of the global South. *Geoforum*, 64, 229-237.
- Téléfonica. (2020). Transparency in Communication Retrieved from <https://www.telefonica.com/documents/153952/183394/Report-Transparency-Communications-2018.pdf/4f05af2f-1542-485f-ca5e-bb50da4a7468>
- Telia, C. (2020). Form For Assessment and Escalation Freedom Of Expression & Surveillance Privacy. Retrieved from https://www.teliacompany.com/globalassets/telia-company/documents/sustainability/template-foe-assessments-and-escalation_march2020_withcommentforpublicversion.pdf
- Tracy, S. J. (2010). Qualitative quality: Eight “big-tent” criteria for excellent qualitative research. *Qualitative inquiry*, 16(10), 837-851.
- Tsui, L. (2015). The coming colonization of Hong Kong cyberspace: government responses to the use of new technologies by the umbrella movement. *Chinese Journal of Communication*, 8(4), 1-9.
- Tuppen, C. (2016). Opening the lines. A call for transparency from governments and telecommunications companies. Retrieved from https://globalnetworkinitiative.org/wp-content/uploads/2016/10/GNI_OpeningtheLines.pdf
- Ulrich, P. (2008). Integrative economic ethics: Foundations of a civilized market economy. Cambridge Cambridge University Press.
- Umberg, T., & Warden, C. (2014). The 2013 Salzburg Workshop on Cyber Investigations: Digital Evidence and Investigatory Protocols. *Digital Evidence & Electronic Signature Law Review*, 11, 128.
- UN. (1948). Universal Declaration of Human Rights. General Assembly
- UN. (1966). International Covenant on Civil and Political Rights. General Assembly
- UN. (2011). UN Guiding Principles on Business and Human Rights. Human Rights Council
- Uppendra, B. (2016). Human rights responsibility of multinational corporations, political ecology of injustice: Learning from Bhopal thirty plus? *Business and Human Rights Journal*, 1(1), 21-40.
- Van Es, K., & Schäfer, M. T. (2017). The datafied society. Studying culture through data. Amsterdam: Amsterdam University Press.
- Veale, M., Binns, R., & Edwards, L. (2018). Algorithms that remember: model inversion attacks and data protection law. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2133), 20180083. doi:<http://dx.doi.org/10.1098/rsta.2018.0083>
- Vodafone. (2020). Correct use of telco data can help in this crisis [Press release]. Retrieved from <https://www.vodafone.com/covid19/news/correct-use-of-telco-data-can-help-in-this-crisis>
- von Krogh, G. (2018). Artificial intelligence in organizations: New opportunities for phenomenon-based theorizing. *Academy of Management Discoveries*, 4(4), 404-409.
- Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer law & security review*, 34(3), 436-449.
- Wagner, B. (2018). Ethics as an Escape from Regulation: From ethics-washing to ethics-shopping? In E. Bayamlioglu, I. Baraliuc, L. Janssens, & M. Hildebrandt (Eds.), *Being Profiling. Cogitas Ergo Sum*. Amsterdam: Amsterdam University Press.
- Webb, A. (2019). The big nine: How the tech titans and their thinking machines could warp humanity. New York Public Affairs
- Weick, K. E. (1988). Enacted sensemaking in crisis situations. *Journal of management studies*, 25(4), 305-317.
- Weick, K. E. (1995). Sensemaking in organizations (Vol. 3): Sage.

- Weick, K. E. (2010). Reflections on enacted sensemaking in the Bhopal disaster. *Journal of management studies*, 47(3), 537-550.
- Weick, K. E., & Sutcliffe, K. M. (2001). *Managing the unexpected* (Vol. 9): San Francisco: Jossey-Bass.
- Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the process of sensemaking. *Organization science*, 16(4), 409-421.
- Weiss, M. A., & Archick, K. (2016). US-EU data privacy: from safe harbor to privacy shield. Congressional Research Service Retrieved from <https://fas.org/sgp/crs/misc/R44257.pdf>
- Weissbrodt, D., & Kruger, M. (2003). Norms on the responsibilities of transnational corporations and other business enterprises with regard to human rights. *American Journal of International Law*, 97(4), 901-922.
- Wettstein, F. (2009). *Multinational corporations and global justice: human rights obligations of a quasi-governmental institution*. Stanford: Stanford University Press.
- Wettstein, F. (2015). Normativity, ethics, and the UN guiding principles on business and human rights: A critical assessment. *Journal of Human Rights*, 14(2), 162-182.
- Wettstein, F. (2016). From Side Show to Main Act: Can Business and Human Rights Save Corporate Responsibility. In D. Baumann-Pauly & J. Nolan (Eds.), *Business and human rights: From principles to practice* (pp. 77-87). New York: Routledge.
- Wettstein, F. (2018). Social responsibility. In E. K. Heath, Byron; Marcoux, Alexei (Ed.), *The Routledge Companion to Business Ethics*. London: Routledge.
- Wettstein, F., Giuliani, E., Santangelo, G. D., & Stahl, G. K. (2019). International business and human rights: A research agenda. *Journal of World Business*, 54(1), 54-65.
- Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaizunas, E., Mathur, V., . . . Schwartz, O. (2018). *AI Now Report 2018*. Retrieved from https://ainowinstitute.org/AI_Now_2018_Report.pdf
- Whittaker, Z. (2020). US tech giants halt Hong Kong police help. Retrieved from <https://techcrunch.com/2020/07/06/facebook-whatsapp-hong-kong-data/>
- Wingfield, R., Tuta, I. T., & Bansal, T. (2020). The Tech Sector And National Action Plans. Retrieved from <https://www.humanrights.dk/publications/tech-sector-national-action-plans-business-human-rights>
- Woods, A. K. (2017). Mutual Legal Assistance in the Digital Age. In D. Gray & S. E. Henderson (Eds.), *The Cambridge Handbook of Surveillance Law* Cambridge: Cambridge University Press.
- Woods, L. (2017). The Investigatory Powers Act 2016. *European Data Protection Law Review*, 3, 103-105.
- Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, 19(3), 321-332.
- Zevenbergen, B., Mittelstadt, B., Véliz, C., Detweiler, C., Cath, C., Savulescu, J., & Whittaker, M. (2015). Philosophy meets internet engineering: Ethics in networked systems research.(GTC workshop outcomes paper). Paper presented at the GTC Workshop Outcomes Paper)(September 29, 2015).
- Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(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.

Curriculum Vitae

Isabel Laura Ebert

Academic Career and Education

October 2020 - now Post-Doctoral Researcher, Institute of Business Ethics, University of St. Gallen

PhD University of St. Gallen, Switzerland, supervised by Prof. Florian Wettstein, University of St. Gallen and Prof. Gina Neff, University of Oxford

February 2017-October 2020 Research Associate and Ph.D. candidate, Institute Business Ethics, University of St. Gallen, Switzerland, Swiss National Sciences Foundation NFP75 Research Project on “Big Data or Big Brother? Big data HR control practices and employees' trust in the employer” (March 2018-April 2020)

Visiting PhD researcher Oxford Internet Institute, University of Oxford (Michaelmas 2019 – Trinity 2020)

October 2012 - September 2014 Master of Arts, International Studies, Peace and Conflict Management, University of Frankfurt, Germany; New York Model United Nations Delegation, University of Frankfurt

October 2008 – September 2011 Bachelor of Arts Politics and Management, University of Konstanz, Germany; Sciences Po Paris France (2010-2011)

Professional Experience

July 2020 - now United Nations Human Rights, B-Tech Project Strategic Advisor

October 2014 – May 2017 Business & Human Rights Resource Centre, London, UK
German language region representative (2014-2015), EU representative (2015-2017)

Internships during BA and MA studies Internships at the Governing Mayor of Berlin, Senate Chancellery of Cultural Affairs (March 2010-August 2010); German Embassy in Pretoria, South Africa (January 2012-April 2012); Goethe Institute New York City, USA (June 2012-September 2012)
