# How is Privacy perceived in German Police Law? Rethinking Counterterrorist Policy in North-Rhine Westphalia.

**Jonas Bradtke**[1]

ABSTRACT

By December 2018, Germany's biggest state, North-Rhine Westphalia (NRW) introduced its revised police law (PolG NRW). The PolG NRW enables previously forbidden surveillance practices to combat terrorism in Germany. Discussion surrounding the PolG NRW revolved around surveillance practices enabled through the law. By using a privacy taxonomy, developed by Daniel J. Solove (2010) this thesis has categorised, analysed and evaluated six sections of the PolG NRW with regards to infringements upon privacy. This thesis (1) identifies potentially harmful activities for personal privacy within the PolG NRW and (2) chases back shortcomings to an incomplete understanding of privacy. Thereby, this thesis suggests that future policy crafting must consider processes that follow the collection of information as potentially harmful activities. By limiting privacy risks to information gathering, activities that belong to information processing and distribution remain largely unregulated, putting the individual at serious risk.

## 1. Introduction

The distinction between the public sphere and the private sphere has been one of the grand dichotomies of western thought since the classical antiquity (Papathanassopoulos, 2015). Aristotle already distinguished between the *polis* (the public sphere of political activity) and *oikos* (the private sphere associated with family and domestic life). The modern understanding of privacy is rooted in the Enlightenment, more specifically in the writings of Thomas Hobbes and John Locke (Regan, 1995). Later, Jürgen Habermas distinguished between the *lifeworld* (intimacy and family) and the *public sphere* (communicative networks that enable private persons to take part in culture and the formation of public opinion) (Papathanassopoulos, 2015). To som, privacy is physical space (see: Aristotle); to some the privacy is a sphere of information that is largely detached from physical locales (see: Thompson, 2010). Different understandings of privacy have shaped citizenship, politics and society in liberal democracies in the west (see: EU Commission: GDPR, 2018). Hence, privacy is understood differently according to various theories and disciplines. In a changing social, cultural and technological background, privacy appears not as a static concept, but rather has a dynamic component (Papathanassopoulos, 2015).

After the attack on the two World Trade Centres in 2001, global terrorism has increasingly threatened the security of liberal democracies in the west. In order to combat terrorism, western governments have continuously expanded – and invested in – surveillance practices (Lyon, 2001; Turnage, 2007 et al). The PRISM programme, leaked by Edward Snowden in 2013 comes to mind. These developments caused scholars, journalists as well as politicians to debate whether expanding counterterrorist surveillance acts as a threat to privacy rights (Lyon, 2001, Turnage, 2007, Solove, 2010

[1] Jonas Bradtke received a bachelor degree in Arts & Culture at Maastricht University in 2019. At the moment he pursues a Master in History at the Heinrich Heine University in Düsseldorf, Germany. Contact: Jonas.bradtke@outlook.de

et al). In return, an old question came up again: what exactly is privacy? What exactly is hurt by state surveillance?

## 1.1 PolG NRW

By December 2018, Germany's biggest state, North-Rhine Westphalia (NRW) introduced a revised police law (PolG NRW). The PolG NRW enables previously forbidden surveillance practices to combat terrorism in Germany. A similar, even stricter law has been introduced in Bavaria in 2018, causing approximately 30,000 to 40,000 people to protest against it (Schnell, 2018). When proposed in NRW, an initial draft, proposed in summer of 2018 was deemed 'anti-constitutional' (WDR, 2018). Among others the police labour union voiced their concerns regarding vague terminology that allows a too broad interpretation of certain sections (Polizeigewerkschaft NRW, 2018). The initial draft was revised and finally introduced by December of 2018. Under revision of SPD the law was announced to be corrected and labelled an important step to fight terrorism in Germany. Activists and scholars remained critical about the bill (Gusy, 2018; Amnesty International, 2018).

The PolG NRW has attracted extensive media coverage (see: WDR, 2018; Süddeutsche Zeitung, 2018) but received very little scholarly attention by legal scholars (see: Gusy, 2018). In both cases, focus of the discussion was on *surveillance practices* enabled through the law. This paper, however, argues that the central problem of the PolG NRW roots in an incomplete *comprehension of privacy*. The adoption of the PolG NRW raises important questions about how privacy is perceived in counterterrorist initiatives. An imminent security threat often trumps privacy concerns, since risks often appear distant and blurry (Solove, 2010). But why is that the case? Why does privacy appear to be at odds with security in case of counterterrorist initiatives such as the PolG NRW? If a scholarly notion of privacy forms different attitudes towards privacy, so does a policy in case of the PolG NRW. In order to grasp privacy issues it is of crucial importance to come to clear terms with what exactly the notion of privacy is that Germany employs. Although it remains of crucial importance to study surveillance practices, this thesis argues to consider that certain conceptions of privacy enables and facilitates problematic activities of surveillance. Thus, this thesis will devote its attention to the pressing question: how is privacy perceived in the PolG NRW?

I will show that identified issues of the PolG NRW can be traced back to a narrow and incomplete understanding of privacy in both (1) the PolG NRW as well as (2) the constitutional limitations placed upon surveillance practices that ought to protect the private sphere of the citizen. For future policy crafting, I will thereby suggest to consider a variety of issues that have not yet been legally recognised by Germany as privacy threats

The first chapter of this thesis discusses different scholarly attempts made to conceptualise privacy. It is crucial to first establish on behalf of which criteria I will evaluate the PolG NRW. I will do so by borrowing from Daniel J. Solove's ''Understanding Privacy''(2010). Throughout his book Solove (2010) provides a concise, yet thorough overview over the most important conceptualisations of privacy. The second chapter introduces the theoretical framework of choice for this paper. Chapter two both (1) explains and justifies the usage of a privacy taxonomy to evaluate the policy at hand as well as (2) provide insight into inclusionary as well as exclusionary mechanisms that determined the content of the case study. In the third chapter of this work, I will devote my attention to the PolG NRW as well as constitutional limits placed upon surveillance practices by the German Constitution. Afterwards, chapter four introduces the contents of the chosen case study. Following, chapter five applies the previously

established taxonomy of privacy to the case study to both identify the conception of privacy employed throughout the PolG NRW and its shortcomings. Finally, chapter six presents the results of my analysis.

# 2. Privacy, a Concept in Disarray

## 2.1 Focus and Selection of Theories

Before diving into the review of scholarly work it must be acknowledged that this review comes with certain limitations. One could fill entire books about the discussion surrounding privacy from the dawn of western civilisation. Hence, a complete, ground-up discussion of accounts made greatly extends the scope of this thesis. This chapter will borrow from the work of Daniel J. Solove (2010). Solove did not only provide a highly valuable account on how privacy has been conceptualised but also developed a highly useful analytical framework to consider infringement upon privacy. Chapter two will discuss the analytical framework in greater detail.

It is of crucial importance to both explore present theories and their shortcomings as well as to settle on a general understanding of privacy that allows me to work out the understanding of privacy employed by the PolG NRW. Scholars like Taylor (2017) have recognised that ''the concept of privacy is difficult to define because it is exasperatingly vague and evanescent, often meaning strikingly different things to different people'' (Taylor, 2017, p. 4). Traditionally, philosophers, jurists, sociologists and scholars of other disciplines have attempted to locate essential elements of privacy common to the aspects of life that we deem private (Solove, 2010). Naturally, conceptualisations that have been worked out greatly differ in reasoning and conclusion. In order to judge on the perception of privacy employed by the PolG NRW it is first important to settle on behalf of which criteria this thesis will speak about the concept of privacy. The conducted scholarly work can be broadly divided into 5 theories. After reviewing these theories, this chapter will work out a general model that allows me to recognise what different models of privacy focus on and value.

### I: Privacy is the Right to be let Alone

Privacy as a 'right to be let alone' is perhaps the oldest and most famous formulation of a right to privacy. It was first expressed in a legal article from 1890 by Samuel Warren and Louis Brandeis. They argue for the legal recognition of a right to privacy in light of new technological developments that were posing a threat to privacy. By 1890, the first commercial cameras allowed everyone, not just professionals to capture pictures (Solove, 2010). The sensationalised press could invade precincts of private and domestic life. Hence, Warren and Brandeis proposed a common law that secure to each individual the right of determining to what extent his or her thought, sentiments and emotions shall be communicated to others (Solove, 2010). By 1890 common law could only protect from defamation, which would protect the reputation. A law of privacy, on the other hand, would protect the individual from ''injury to the feelings'' (Solove, 2010, p. 16).

Although convincing at first glance, their account on privacy comes with serious limitations. Privacy is viewed as a type of immunity and exclusion. If privacy is merely being left alone, any human interaction could be labelled a violation of personal privacy (Solove, 2010). Additionally, both Warren and Brandeis never formulated what privacy *essentially* is. Hence, privacy as the right to be let alone appears too general to use as an analytical tool for my case study.

II: Privacy is Limited Access to the Self

The first theory of privacy illustrated that this thesis is in need of a more detailed, yet generally applicable approach on privacy. Perhaps viewing privacy as 'limited access to the self' is a more fruitful approach. This conception of privacy details the ability to shield oneself from unwanted access by others. Scholars have labelled it a more sophisticated version of the right to be let alone (see: Solove, 2010). The 'limited access theory' incorporates freedom from government interference as well as intrusions by the press and others. What it does better than the previous theory is that it extends privacy beyond merely being apart from others. Hence, scholars like O'Brien (1981) consider a variety of agents that could possibly infringe upon people's privacy. Nevertheless, this approach does not describe which matters are private, only that one should be able to independently decide to disclose or not to disclose information. A right to privacy as 'limited access to the self', entitles the individual to exclude others from (a) watching, (b) utilizing, (c) invading one's private realm (Solove, 2010).

While this approach certainly provides more detail about what kind of activities are harmful to individual privacy, it never defines what matters are private. Additionally, it is not clarified which degree of access constitutes a privacy violation. These shortcomings were addressed by scholars like Ruth Gavison (2012) in an attempt to modify the limited access theory. Gavison expanded that limited access consists of (1) secrecy, (2) anonymity, and (3) solitude (Solove, 2010). Daniel Solove (2010) rightfully pointed out that even if one would expand the limited access theory, it restricts privacy to matters of withdrawal (solitude) and concealment (secrecy, anonymity). Additionally, invasions into private affairs such as harassment and nuisance ''and the governments involvement in decision regarding one's body, health, sexual conduct, and family life'' are excluded as harmful activities in this theory (Solove, 2010, p. 21).

III: Privacy is a Derivative Right

The latter two theories argue that privacy is rather a form of self-interested economic behaviour, concealing harmful facts about oneself for one's own gain. However, both theories fail to either define (1) what content constitutes a private matter or (2) what privacy really is. Per Thompson (1975), the right to privacy is composed out of a subset of other rights. Hence, it is derivative, i.e. ''not standalone, but rather part of a cluster of rights which make up a general right'' (Taylor, p. 5, 2017). The rights in the cluster do not have a lot in common. Nevertheless, they share that they relate to privacy. Thompsons notion of privacy is illustrated through thought experiments which are meant to exemplify the interconnectedness of the cluster of rights. For example, Thompson identifies property rights to intersect with the right to privacy. After all, personal information is personal property. Hence, to illegally acquire information is both harming property rights and, in return, privacy rights. Thompson presents a useful switch of focus: away from abstract theoretical interests towards activities that harm privacy. However, it is implied that all concerns of privacy, thus, must be grounded on other, derivative, rights. Nevertheless the interest identified by the author remains singular. If privacy is derivatively protected, the interest must also be scattered. Hence, Thompson's approach does achieve to incorporate the variety of understandings of privacy but limits itself with only possible singular interest in privacy. Thompson rightfully acknowledges that her model is not a definitive conceptualization, but rather a simplification worth having. But what if there is a pure interest behind privacy that does not ground on existing property rights?

IV: Privacy is Control

Andrei Marmor (2015) conducted a thought experiment to get closer to what interest constitutes privacy. Marmor envisions a global panopticon where everything is there for anyone to see, hear or smell. If a transition into such a world would happen without harming other, derivative rights one would still not want to live in such a society. Hence, there must be a distinctive interest which underlies privacy rights that does not ground on other rights. The interest is precisely to keep certain facts about oneself hidden from other people, in order to have *control* about how others view us (Taylor, 2017). A control interest acts strong enough to ground an interest in privacy without intersecting with derivative rights, as per Thompson (1975). Nevertheless, focusing on control implies secrecy. Marmor's focus on secrecy fails to recognise that individuals want to keep things private from some people but not from others. Control theory, as per Marmor, emphasizes on limitless disclosure. However, sometimes we do not desire complete secrecy but rather confidentiality, which consists of sharing the information with a select group of trusted people (Solove, 2010). Additionally, not all activities we deem private occur behind closed doors. These activities and sentiments are not secrets but we still view them as private matters, e.g. the books we read, the product we buy. All in all, the secrecy theory views privacy as opposed to publicity, which does not apply to all private matters.

V: Privacy is Power

In a similar vein, Lever (2013) and De Bruin (2010) identified that an interest to prevent power inequalities must lie at the heart of privacy concerns. An individual who has acquired information over another individual is likely to stand in a position of power over that individual. Naturally, the individual at stake has no interest in this. Blackmailing, for example, provides the extortioner with sufficient power over the individual at stake to demand certain things. Even further, others having information might also compromise autonomy. After all, being able to make choices independently – free from manipulation of others – is probably the most important precondition of an autonomous life (Taylor, 2017). Knowledge that someone has information will already set back the individual's interests. The thought that a certain agent, or entity, might interfere will cause one to make measure to pre-empt this, at great cost to one's autonomy. Lever (2013) and De Bruin (2010) have made important contributions to the impact of privacy violations on autonomy and behaviour in a democratic society. The authors provide valuable insight on the consequences of privacy infringements on autonomy and deliberative capabilities. However, grounding privacy interest on power appears to be not sufficient to conceptualise privacy. Similar to Marmor's theory (2015) the work of Lever (2013) and De Bruin (2010) boils down to a control interest. While privacy invasions certainly enable the invader with substantial power, control theory again fails to define which kind of information can act as powerful when used against the individual. Thus, any information can act as powerful. Hence, the most interpersonal contact in society would constitute a privacy invasion. However, we are frequently seen and heard by others without perceiving this as even the slightest invasion of privacy (Solove, 2010).

## 2.2 A Switch of Focus

Traditional approaches of privacy often are presented either too narrowly or too vaguely. Existing research often regards privacy as a ''unitary concept with a uniform value that is unvarying across different situations'' (Solove, p.8, 2010). All scholars that have been discussed refer to intersecting or

underlying interests that, when harmed, harm privacy rights. However, debating interests appears to either paint a too narrow picture which excludes other important interests or a too broad picture, which presents itself too generally to apply it to the case study of this thesis. Hence, the traditional way to locate the essential, core characteristic of privacy appears to be insufficient for the task of this thesis.

The previous sections have illustrated that although privacy is seen as the 'heart of our liberty' it is still very much a concept in disarray. Different conceptions often clash, causing privacy problems to not be well articulated. As Robert Post put it: ''privacy is so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings that I sometimes despair whether it can be useful at all'' (Solove, p. 2, 2010). Perhaps one should switch the focus entirely when conceptualizing privacy.

Borrowing from Ludwig Wittgenstein's notion of 'family resemblances', Daniel J. Solove (2010), professor of law at the Washington University law school, characterised privacy to be a concept without single common characteristics. Yet, it draws from a common pool of similar elements. This is very much connected to the purpose of privacy rights. When a state legally protects privacy, the state protects its citizens against disruptions to certain activities. A privacy invasion interferes with the integrity of certain activities and even destroys or inhibits some activities. Thus, privacy's value emerges not from itself, but from the activities it protects. This approach situates itself rather close to Thompson's (1975). Both theories steer away from underlying interest and focus on harmful activities that might hurt privacy. Both argue that privacy involves a cluster of protections against a group of different but related problems Yet, Solove (2010) manages to incorporate a variety of activities, while Thompson limits herself to only derivative legal rights. Solove suggests that privacy should conceptualised by focusing on the specific types of disruption rather than locating a common denominator of these activities. Focusing on a multitude of potentially harmful activities allows Solove's framework to move the discussion surrounding privacy from the vague term of privacy toward specific activities that pose privacy problems. These problems impede valuable activities that society wants to protect, and therefore society devices ways to address these problems. Because Solove's model allows one to analyse privacy issues from activities rather than core interests, it presents itself sufficient to apply to the PolG NRW, to analyse what kind of activities are permitted and protected. The following chapter will further develop Solove's framework.

# 3. Methodology

As suggested in chapter one, it might be best to not focus so much on the core interest behind privacy, but rather to identify when privacy is at stake to get to the root of privacy problems. Daniel J. Solove (2010) has done so by developing a taxonomy to assess and categorise policies on behalf of privacy invasions.

## 3.1 A Taxonomy of Privacy

All taxonomies are generalisations based upon a certain focus. Solove's taxonomy aims to aid the crafting of law and policy (Solove, 2010). Within policy analysis, employing a taxonomy is a rather unusual tool. Most policy categorisation is done by typology. Typologies have long been used in political science, since they allow to conceptually separate a given set of items multidimensionally. A taxonomy, on the other hand, classifies items on the basis of empirically observable and measurable characteristics

(Smith, 2002). At first glance, empirical qualities of policies are not immediately apparent. Nevertheless, a number of scholars have suggested that employing a taxonomy might bear the possibility to discuss morality polices, i.e. policies that strike up debates grounded on values (Smith, 2002; Marradi, 1990). Even though empirically observing policy might appear odd to some, policy is a social construction and, thus, rooted in individual perceptions. Ideology, for example, is a mental construct that is routinely measured and accepted to have predictive qualities (Smith, 2002). Hence, employing a taxonomy allows me to have a multi-dimensional model of classification to test the case study.

The model begins with the *data subject*, i.e. the individual whose life is most directly affected by the activities classified in the taxonomy. Various entities (other people, businesses and the government) *collect information* from the data subject. Information collection acts as the first of four stages in Solove's taxonomy. For every stage, Solove details a number of harmful activities that belong to said cluster. In case of the first stage, Solove identified (1) surveillance, i.e. the watching, listening or recording of an individual's activities and (2) interrogation, i.e. the questioning or probing for information, to be harmful activities.

Those who collected the data, to which I shall refer to as the *data holders*, then *process the information*. In practice, processing details the storing, combining, manipulating and using of data. Information processing acts as the second stage of the taxonomy. Harmful activities in this cluster are (1) aggregation, i.e. the combination of various pieces of data about a person, (2) identification, i.e. linking information to particular individuals, (3) insecurity, i.e. carelessness in protecting stored information from leaks and improper access , (4) secondary use, i.e. use of collected information for a different purpose than intended without consent of the data subject and (5) exclusion, i.e. the failure to allow the data subject to know about the data that others have about himself or herself and its handling and use.

Finally, information is disseminated, i.e. the data holders transfer the information to others or release the information. Identified harmful activities in this cluster are: (1) breach of confidentiality, i.e. breaking a promise to keep personal information confidential, (2) disclosure, i.e. revelation of truthful information about a person that affects the way others will judge the data subject's reputation, (3) exposure, i.e., revealing another's nudity, grief or bodily functions, (4) Increased accessibility, i.e. amplifying the accessibility of information, (5) blackmail, i.e. the threat to disclose information, (6) appropriation, i.e. the use of the data subjects identity to serve another's aims and interests, (7) distortion, i.e. disseminating false or misleading information about individuals. Fig. 1 visually illustrates the process covered by the taxonomy.

This process has to be understood to chronologically illustrate the data moving further away from the data subjects control. These three stages (collection, processing, dissemination) act as three categories in Solove's taxonomy that each contain a number of potentially harmful activities (see: Fig. 1). Invasions acts as a fourth activity and include infringements directly on the data subjects privacy. Instead of progressing away from the data subject, invasions progress towards the individual. The taxonomy acts as a bottom-up description on the kinds of privacy problems that are addressed in discussions surrounding privacy law, constitutions and guidelines (Solove, 2010). The following section details the content of the case study to which the taxonomy will be applied.

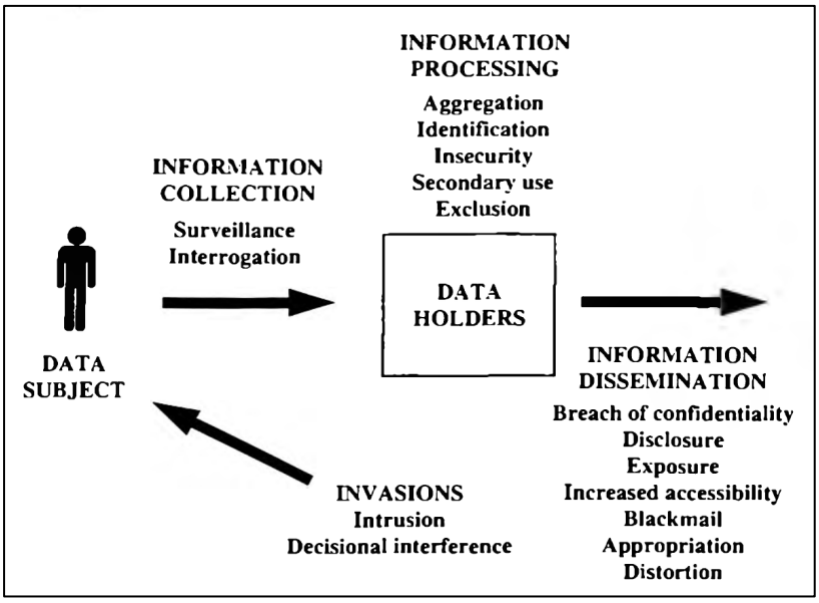


*Figure 1*.
Model of taxonomy. (Solove, 2010, p.104)

## 3.2 Case Study and Limitations

The PolG NRW entails 46 pages of regulations. Thus, it was inevitable to place inclusionary and exclusionary criteria on which paragraphs will be analysed through Solove's model. This work will limit itself to sections that (1) aroused special attention in politics and media as well as (2) paragraphs that are occupied with the three stages of data gathering identified by Solove (2010). Ultimately, these criteria produced six sections that check both criteria. This work will limit itself to § 20c (Fn 19), § 22 (Fn 5), § 22a (Fn 22), § 23 (Fn5), § 26 (Fn 21) and §27 (Fn 21). For the sake of clarity, I will now briefly detail the content of the paragraphs in question. § 20c is occupied with the gathering of data through surveillance of ongoing telecommunication. § 22 deals with the storage of gathered data, while § 22a describes the processing of personal data. § 23 expands on § 22a and details processing of personal data for different purposes than intended. § 26 outlines general rules for distribution of personal data. Finally, § 27 details this notion further and describes distribution of personal data across German state borders. The paragraphs at hand deal with either *information gathering* (§ 20c), *information processin*g ( § 22, 22 a, 23, 24a), or *information distribution* (§ 26, 27). These three generalisations reflect upon three different stages in data handling and collection, which Solove (2010) identified to bear potential risks for privacy.

Although the focus of this work lays primarily on the PolG NRW it was necessary to discuss overarching regulations of privacy as stated in the German Constitution. In Germany, the 'Kernbereich privater Lebensgestaltung' [core area of private life style] ultimately determines what is perceived as an intrusion into the private sphere. I shall refer to the Kernbereich privater Lebensgestaltung only as 'KPL' from now on. Because the KPL provides valuable insight into the understanding of privacy employed throughout the analysed sections of the PolG NRW, it will also be included in the case study.

The following chapter will first devote its attention first to an outline of the KPL. Afterwards, an outline of the six paragraphs in question will be provided. In chapter five, the core analysis will work out

the qualities and shortcomings of both cases to get closer to the privacy conception employed in the PolG NRW.

# 4. Exploring the Case Study

## 4.1 Constitutional Limitation: The Kernbereich privater Lebensgestaltung

Any surveillance conducted in Germany must conform to the standards of the KPL which is deemed to be the most private sphere of living in Germany. Hence, the understanding of what constitutes privacy in Germany is largely based on this notion.

The idea of a realm, untouchable by the state – a sphere of human freedom – is a key component of liberal reasoning of the 19th century. Otto von Gierecke, renowned German legal and political scholar of the 20th century, famously argued that to be human is not to be citizen. Being citizen should merely constitute one part of a personality. Hence, society was in need of an untouchable right to individual freedom. This idea was implemented into German legislation by 1957 (Baldus, 2008). New legislation introduced that the citizen is able to retreat into a sphere of human freedom, and private life: the 'Kernbereich privater Lebensgestaltung'. By 1996, discussions surrounding residential surveillance expanded the KPL. It was declared that even in light of overwhelming interest of the general public, the KPL must remain untouched by the state. A further expansion took place by 2004. It was added that within the KPL there must be the possibility for the individual to express inner processes and reflections without fear of state surveillance (Baldus, 2008). Since 2004 the KPL has remained largely untouched and still acts as the most private a citizen can legally be in Germany. Allow me now get into greater detail about what exactly constitutes the KPL.

The KPL allows to express inner reflections, emotions and experiences of very personal nature, expression of sexuality, as well as sub-conscious experiences. Whether something classifies to be in the realm of the KPL is a question of whether the content of a conversation or monologue is of ''höchstpersönlicher Art'' [deeply personal character] (Baldus, 2008, p. 219). Additionally, it must be considered whether the *content* is in touch with other, more public, spheres of living and whether the content is in touch with matter of general relevance. However, this does not suggest that the KPL is only constituted if an individual is by itself. Moreover, a situation can be a matter of the KPL in which an individual is in communication with others. Since the KPL is rooted in core elements of personality, law has acknowledged that social relationships are an essential part of the KPL. Family members, persons of special trust (e.g. lawyer, psychologist, doctor) can be a part of the Kernbereich privater Lebensgestaltung (Baldus, 2008). Even highly personal matters of non-communicative kind, e.g. diaries, are also included in the KPL. So far, both individuals involved as well as content of conversation or monologue act as indicators whether a situation specifies to belong the KPL. Spatiality, however, also plays an important role. Hence, a conversation at the workplace would not classify as a matter of the KPL, since the place implies association with the social sphere. In case the space might be a place of retreat and the persons that communicate are part of the inner circle, or persons of special trust, the content of the conversation would still determine whether that conversation is part of the KPL (Baldus, 2008).

The individual would lose its protection of the KPL if content of a conversation would reflect imminent or past crimes. Hence, although it is constitutionally manifested that the KPL acts as an

isolated untouchable private sphere, this does not imply that the state has to restrain from any interference. The German state is allowed to read through private diaries, or to conduct residence or telecommunication surveillance. However, the state is not allowed to take the risk of potentially harming the KPL, if certain indicators show that the state will penetrate the sphere of the highly personal. This implies that if authorities want to conduct surveillance, they would have to make a prognosis beforehand whether the operation will harm the KPL (Baldus, 2008). If the answer is yes, authorities have to restrain from surveillance (duty of omission). If the operation is claimed to not hurt the KPL but does so regardless, the operation has to be cancelled immediately (ending obligation). Additionally, all gathered data has to be deleted (deletion obligation). In case data that is associated with matters of the KPL has been gathered, it can under no circumstances be use (denial of processing). A neutral instance will judge on this behalf (Baldus, 2008). Now that the framework within which any surveillance in Germany can take place has been explored, the following section will deal with the content of the PolG NRW.

## 4.2 The PolG NRW: Contents in Question

Changes to the NRW Police Law were first announced in June 2018. Swiftly, the proposed changes and allegedly vague terminology caused NRW privacy appointees as well as Amnesty International to express worries about the draft (Amnesty International, 2018). By December 2018, a revised draft was implemented into the general police law of NRW. Both ruling parties (CDU, FDP) as well as the SPD voted for the draft. The local government stated that problematic sections and formulations concerning constitutional rights and privacy have been revised under supervision of the social democrats in order to present a more balanced revision of the law. Nevertheless, critics noted that only few of the problematic sections were changed for the better (Amnesty International, 2018).To effectively analyse the sections in question it is first best to outline contents of the paragraphs. Structurally, the paragraphs will be discussed according to the analytical model introduced in chapter two. *Table 1* provides an overview of the organisation of paragraphs.

*Table 1*

| | |
|---|---|
| Information Gathering | § 20c |
| Information Processing | § 22, § 22a, § 23, § 24 |
| Information Distribution | § 26, § 27 |

### 4.2.1 Information Gathering: § 20c – Datenerhebung durch die Überwachung der laufenden Telekommunikation [Data gathering through surveillance of ongoing telecommunication] (PolG NRW, 2019, p. 18)

So far, the NRW PolG has not entailed a regulation for telecommunication surveillance (Gusy, 2018). By new standards, dedicated 'Informationsmittler' [information investigators] are appointed. Section two of § 20c expands on this notion. Information gathering does to remain limited to telecommunication. With the newly introduced law, information technology acts as an additional source of information. Hence, computers, laptops as well as smartphones can be surveilled as well. This is rather close to the concept of 'online frisking', which before was only possible under special circumstances (Gusy, 2018). In order to get involved in telecommunication surveillance, the investigator has to present evidence. Such an appeal needs to include: (1) name and address of the data subject, (2) either telephone number or information

on the information technology device in question (including manufacturer and software), (3) the kind, extent and duration of the surveillance, (4) the possible crime as well as (5) a justification of why surveillance measures like these must be employed. Said evidence has to express that the data subject in question poses a threat or *is close to* pose a threat. When conducting surveillance, the investigator has to document identification of the information technology system as well as alterations made within the system. § 20c also comes with a number of limitations. Both surveillance of telecommunication as well as information technology is limited to ongoing communication. Surveillance is only allowed so far as it does not enter the 'Kernberreich privater Lebensgestaltung''. All surveillance under § 20c is impermissible once gathered data touches upon the KPL of the data subject. Additionally, the investigator is obligated to protect data from unwanted altering of contents and unwanted deletion.

4.2.2 Information Processing: § 22: Datenspeicherung, Prüfungstermine [Data storing, Scrutiny] (PolG NRW, 2019, p. 20)

Once personal data are gathered, the police can save both physical and digital data, if the data will be relevant for future investigation. Starting with the first new year after the last bit of data was collected, both automatically as well as manually gathered data can be saved at a maximum of ten years. After ten years, the data will be scrutinised again and it will be determined whether it is necessary to leave the data assessable and searchable in the system. All gathered data must be deleted if the data subject is proven innocent by court. Individuals that are in touch with a potentially future criminal data subject can also be surveilled. Their data will can be saved up to one year until it must undergo an inspection. All data can be combined, altered and used if necessary to fight crime.

Information Processing: § 22a: Verarbeitung besonderer Kategorien personenbezogener Daten [Processing special categories of personal data] (PolG NRW, 2019, p. 21)

Policemen taking part in the surveillance process have to be sensitised to take special care of personal data. Additionally, for the sake of transparency it must be indicated who gathered the data, when it was gathered and if someone has changed it.

Information Processing: § 23: Weiterverarbeitung von personenbezogenen Daten, Zweckbindung, Zweckänderung [Processing of personal data for different purposes] (PolG NRW, 2019, p.22)

Personal data, gathered by the police, can be processed to (1) fulfil the same task as originally intended and (2) to protect the same rights and liberties and to prevent the same crimes. However, the police is also allowed to use personal data for different purpose than originally intended. This is possible if data will assist to prevent and fight crime of similar weight or to protect rights and liberties of similar importance.

Information Processing: § 24: Weiterverarbeitung zu besonderen Zwecken [Processing (of data) for special purposes] (PolG NRW, 2019, p. 22-23)

The police is allowed to use gathered personal data for statistical purposes, if the data was anonymised as early as possible. Additionally, gathered data can be used to train future and present policemen and policewomen. Data must not be anonymised in this case, unless the data subject might have an understandable strong interest to keep his or her data confidential.

4.2.3 Information Distribution: § 26: Allgemeine Regeln der Datenübermittlung, Übermittlungsverbote und Verweigerungsgünde [General rules for data distribution, prohibition of data transmission and refusal] (PolG NRW, 2019, p.23)

The police is allowed to share their gathered data with other police departments. Both data of the data subject itself as well as third party data, i.e. individuals in relation to the data subject, are allowed to be passed on to other police departments. In case of third party data, this is only the case if data from the subject itself and third parties are hard to separate.

Information Distribution: § 27: Datenübermittlung im innerstaatlichen Bereich [Data distribution within the boundaries of Germany] (PolG NRW, 2019, p. 24)

§ 27 expands on § 26 and details the distribution of gathered data across state borders within Germany. Although the newly introduced regulations are only in effect in the German states of Bavaria and North-Rhine Westphalia, the police is allowed to share gathered data across county state borders.

# 5. Analysis: PolG NRW & KPL

The previous chapter described case study in relation to the privacy taxonomy. This chapter will apply the taxonomy of privacy to the case study.

## 5.1 Information Gathering

§ 20c classifies as dangerous activities in one category of the taxonomy, as a surveillance activity. This one certainly is the most obvious. After all, the law refers to itself as a regulation of surveillance practices. Nevertheless, Solove (2010) was right to classify even the most basic surveillance practice as a potentially harmful activity. The possibility that one can be watched persistently can create feelings of anxiety and discomfort. Additionally, it can cause one to alter one's behaviour. Surveillance can lead to self-censorship and inhibition (Solove, 2010). Hence, being watched and listened can act as a tool of social control, enhancing the power of social norms. It is especially surveillance in private settings, as implied by § 20c, that is of great harm to the individual's well-being. Scholars like Lever (2013), De Bruin (2010) and Taylor (2017) have conducted important work on the impact of even the most basic surveillance practices on democratic capabilities. As briefly touched upon in chapter two, the authors argue for robust privacy rights because they are necessary for individuals to form the deliberative capacities necessary to hold powerful agents to account. Only in a private situation groups or individuals can test out arguments and discover common concerns and work out how to best present these concerns to the society at large. Comprising privacy would therefore also compromise deliberative abilities (Taylor, 2017).

In his taxonomy, Solove focuses on continuous monitoring when discussing surveillance and its potential harming character. One could certainly argue that § 20c does not allow *continuous* monitoring of the data subject. This, in return, would mean that harmful consequences outlined by Solove would not apply to this paragraph. Two arguments can be held against this.

Frist, whether it be overt or covert, continuous or selective, surveillance bears harmful impact for the data subject being surveilled. Surveillance demonstrates a lack of respect for its subject as autonomous person (Solove, 2010). Second, § 20c limits itself in the regard that surveillance is limited to ongoing communication. While this limitation is easily applicable to telecommunication, the question

arises to what extent this is applicable to other information technology. After all, it might be a matter of interpretation at which stage a conversation over an online messenger service, for example, starts and when it ends. Christoph Gusy (2018) argues that this section attempts to avoid encryption techniques of online communication services. Self-protection, human dignity and privacy count as basic rights in the German constitution. Gusy rightfully points out that § 20c would legally bypass these rights. After all, the investigator has to prove beforehand that the risk of a crime demands infringing on the data subjects privacy rights. However, how is it possible to determine beforehand whether a violation of privacy is necessary, when the very reason for this violation lies in the content of a conversation that *will* eventually be held?

An investigator would still need a permit to surveil the data subject. However, while § 20c limits itself to the selective surveillance of telecommunication and information technology, § 30 certainly allows the police to access and request data from public institutions that have *continuously* gathered personal data (PolG NRW, 2018, p. 26). Thus, while it is not the state gathering information, the police certainly has access to continuously gathered personal data *without* the compliance of the data subject. Even if that would not be the case, selective surveillance would still constitute harmful consequences for any citizen. Concealed spying on the data subject can in similar regards produce normalising, behaviour altering consequences for the data subject. Already the panopticon, and it's perfectly individualised visibility illustrated that in a state of uncertainty whether the data subject is being watched, the data subject will most likely alter his or her behaviour. Hence, it does not matter whether surveillance is conducted only in special situations or continuously. Since the data subject will not be noticed when being surveilled, as it says in § 20c, everyone could be subject of state surveillance at any given time.

Having inspected § 20c , it becomes apparent that both § 20c and § 30 infringe upon privacy due to the fact that they enable and facilitate continuous as well as selective surveillance. Serious consequences that have to be identified are impact on the data subjects autonomy, democratic capabilities, well-being as well as behaviour. While one might argue that infringements upon privacy are limited to the act of watching and recording, Solove's taxonomy (2010) includes the processing of data to be of potentially harming character. Allow me now to focus on the second cluster of the taxonomy: information processing.

## 5.2 Information Processing

Information processing is occupied with the way information is stored, manipulated and used (Solove, 2010). The investigated paragraphs in the PolG NRW qualify as potential privacy risks in three categories of the taxonomy.

First, paragraphs of the previous section (§ 20c, 30) as well as §22a illustrate that the police is allowed to combine various pieces of data about a person. § 20c allows the police to gather information through both telecommunication as well as information technology devices. § 30 allows the police force to gather information through public institutions. After all, more telling than isolated data is a synergy of information. However, Solove (2010) identified the act of aggregation as a harmful activity to privacy. The image created through aggregated data bears the potential to represent a distorted version of the data subject. People expect certain limits of what is known about them based on where they, willingly or unwillingly, left small pieces of data. Aggregation upsets these expectations because it combinates data in unexpected ways. Aggregated data usually produces relatively accurate estimates. Nevertheless data

is freed from its original context in which it was gathered (Solove, 2010). No precaution is taken in the PolG NRW to pre-empt dangerous consequences of aggregation of data.

Second, § 23 and § 24 detail the possibility to use personal data for other purposes as originally intended: for research purposes and as long as the data will help to fight similar crimes and protect liberties and rights of equal importance (PolG NRW, 2019). Secondary use of personal data must be identified to infringe upon privacy rights. Not only is data collected without consent but also it is used without the consent of the data subject. By law, both the breach into privacy as well as secondary use is justified by an imminent terrorist threat. However, in light of continuous surveillance, the PolG NRW displays a lack of awareness of potential harm caused by secondary use. Of course, measures would be taken in case data is used for research projects. However, anonymisation strategies have evidently failed before. Especially with regards to secondary use for research purposes, the paragraphs in question pose a threat. In 2008, researchers studied the profile data of from Facebooks accounts of college students of a US university. All steps taken to protect the identity of the students failed. Although no names were mentioned throughout the study, the subjects were swiftly identified, putting the privacy of the students at risk (Zimmer, 2010). It was merely small details, such as field of study that allowed other people to identify the university, and following: the students themselves. Again, within the PolG NRW no precaution is taken to protect the data subject from potentially harmful consequences of secondary use.

Third, data is cautiously scrutinised for further storing. As per § 26, data of both the data subject can be stored up until ten years. In case of peers in touch the with the data subject personal data can be saved up to two years. Both without scrutiny. By January 2019, a 20 year old hacker published highly personal data of hundreds of German politicians as well as journalists. Besides personal matters, the leak also included copies of diplomatic passports as well as drafts of political speeches and papers. The hacker employed a variety of methods. Additionally, the highly sensible political material goes to show that the hacker somehow acquired aces to the internal system of the German government (Deutschlandfunk, 2019). This case illustrates that seemingly no system is completely secure. Both individuals interacting with a seemingly secure network as well as network structures themselves always bear a certain degree of vulnerability (Bronk, 2008). Hence, personal data that is stored up to ten years certainly is not safe. Large scale storing of highly personal data will always remain vulnerable to hacking, thus putting the data subject at serious risk. Once a hacker has acquired highly sensible and personal information the data subject can possibly be blackmailed. Hence, data will always remain unsafe once it is stored. Both individuals interacting with the data base as well as the data base itself poses a threat to the security of personal information. Additionally, § 22 does not require investigators to anonymise data.

Having now discussed threats to privacy posed by information processing regulations in the PolG NRW, the following section will discuss whether information distribution practices of the PolG NRW pose a threat to privacy.

## 5.3 Information Distribution

The detailed paragraphs that are occupied with the distribution of information classify as harmful activities in one point of the taxonomy.

§ 26 and §27 amplify the accessibility of information. The paragraphs in question allow the police to share personal data among other precincts and even across county state borders within

Germany. Again, this comes with no surprise. Federal courts in the United States, for example, have long developed system that place their records online (Solove, 2010). An advocate for robust counterterrorist security might argue that personal information about suspects is readily available at local police stations, hence, why not just fasten processes by putting information online? Increased accessibility creates a greater possibility of disclosure, which classifies as a harmful activity as per the employed taxonomy. More access points to sensible, personal data equals more potential security risks for the individual. Hence, amplifying accessibility amplifies risks of disclosure.

## 5.4 Objections and Justifications

A number of conclusions taken from my analysis have been identified before. After all, the PolG NRW marks not the first controversial law, or surveillance practice to combat terrorism in the west (see: Snowden, 2013). Scholars have also worked out a number of justifications for privacy harming security measures. Allow me to discuss two valid arguments that can be held against my findings.

The first justification that renders itself important for my conclusion is the 'lesser evil justification'. This is certainly the most prominent argument to legitimise expanding state surveillance apparatuses post-9/11. Scholars like Himma (2007) or Walzer (2015) argue that even though some violations are in place, the benefits that can be gleamed will outweigh the moral reasons (Taylor, 2017). Hence, when the social costs of respecting privacy rights become too great, policies are justified to ignore them. At first notice, this appears to be very convincing. Of course, every society must exercise a certain degree of control. Britain's CCTV is widely known as a 'friendly eye in the sky, not big brother' since 1961 (Solove, 2015). One cannot oblige police departments to restrain from the exchange of potentially useful information. After all, in case of a manhunt across state borders, the police needs to share valuable information to successfully prevent any harm directed at citizens. Hence, one could certainly argue that § 26 and § 27 of the PolG NRW must enforce a necessary evil to combat terrorism. And in light of a terrorist attack harming the data subjects privacy, appears to be the lesser evil. For this justification, some ground rules have been set by Walzer (2015) detailing when rights must give way for a greater evil. First, the consequence of not violating rights must be significant. Second, the catastrophe must have certain degree of imminence. For example, in the dusk of WW2 allies looked in sight of victory. Hence, infringing upon the rights of German non-combatants was seen as a necessary evil (Taylor, 2017).

In case of the PolG NRW, case one of Walzer's model could be satisfied. It might be an open question whether the degree of security guaranteed through the data collection is large enough. Nevertheless, consequences of a large scale terrorist attack could be tremendous to Germany and its citizens. However, case two of Walzer's model is certainly not satisfied within the PolG NRW. In case of § 20c data is collected from the data subject to figure out whether an attack is happening in the first place, not to go after imminent suspicion. Hence, a lesser evil explanation does not account for the surveillance practices throughout the PolG NRW.

The second justification worth noting for this work is the 'rights forfeiture justification'. Individuals can be thought to lose their rights if they have acted in ways that involves forfeiting those rights. (Taylor, 2017). Consider person A attempting to murder person B. In order to defend him or herself person B hits person A in the head. Under regular terms this would be a criminal offense. But since person A wanted to kill person B, person A has forfeited its right of protection. However, it is not

only through immoral actions that individuals are thought to forfeit their rights. Because all citizens benefit from the product that the state provides, they are under obligation to contribute something towards their production (Taylor, 2017). Both the PolG NRW as well as the KPL employ this justification. And it does appear very convincing with regards to the threat of terrorism. § 20c, § 27, §26 and § 30 as well as the KPL describe a condition under which the police is allowed to penetrate the KPL, or private sphere, of the data subject. It is argued that if a conversation reflects a past or imminent crime, any protection through the KPL becomes invalid. Political justifications made by the SPD, CDU and FDP also detailed that privacy is a cost that it justified through increased security. This, in return, implies that if one benefits from the increased security that a data collection regime generated, one has no right against some of one's own personal data being collected by the regime (Taylor, 2017). However, in case of the PolG NRW, equal extraction of data does not involve equal distribution within Germany. Some will find the given data collection more costly than others, simply because they are less willing to permit their personal data to be used. In addition, different groups of people might have greater or lesser need for security and ensuring fairness might involve adjusting the costs in a number of ways to reflect this (Taylor, 2017).

This work does not argue that any data collection is impermissible by itself. However, given that data collection appears to be neither fairly organised nor democratic, none of the outlined practices in the PolG NRW should be regarded permissible. The two points raised against my argument, hence, prove to not justify data collection, distribution and processing practices raised throughout the PolG NRW. Although they certainly legitimise practices to a certain extent, justifications swiftly appear to be weak. These justifications do not account for an incomplete comprehension of what constitutes a harmful activity to individual privacy.

## 6. Findings

So far, both (1) the Kernbereich privater Lebensgestaltung as well as (2) enabled infringements upon privacy through the PolG NRW have been worked out. What do the identified harmful activities teach about the perception of privacy? Allow me to start with the overarching framework provided by the Kernberreich.

### 6.1 Privacy in the KPL

The KPL reveals a prospective conception of privacy to which any surveillance practice and policy must adhere. Three striking characteristics must be mentioned at this point.

First, although partaking members of a conversation as well as the space of a conversation or monologue is considered in the KPL, it is ultimately the content of a conversation or monologue that will determine whether something is deemed private. Second, the KPL connects privacy to intimacy and vulnerability. The KPL is understood as a deeply personal sphere in which the individual can express and communicate his or her most personal sentiments and emotions. Third the KPL puts strict limitations on state interference in private lives, any limitations and prohibitions to penetrate the KPL will be abolished once national, societal or governmental security is at risk. Both the KPL as well as a number of sections that were previously explored express that privacy is lost if the data subject poses a risk to eventually engage in terrorist activities, for example. This perceptions reflects a common understanding of privacy, especially in light of counterterrorist policies in the 21st century. It appears that privacy and security are

understood as mutually exclusive concepts. Hence, more robust privacy rights can only be introduced on the expanse of national security. In return, stricter security measurements will and must penetrate the KPL to establish and guarantee security.

The KPL provides a valuable insight into what is deemed private and personal according to German law. Following, if the understanding of privacy is flawed and limited within the KPL, so will be the policies in practices. However, the notion implied by the KPL is generally formulated in order to apply it to a variety of cases. The KPL determines which limitations must be placed on surveillance practices and policies. Hence, the KPL only allows to work out an *estimated* conclusion of how privacy is conceptualised in the PolG NRW. The pressing question arises whether detected problems within the limitations that are legally placed upon surveillance practices are reflected in the newly introduced regulations.

## 6.2 Privacy in the PolG NRW

The analysed paragraphs show (1) a flawed understanding of what kind of privacy must be protected, (2) serious infringing upon personal privacy and (3) security risks in the way data is stored and processed.

Firs, the flawed understanding of privacy employed by the PolG NRW can be seen through the second and third cluster of activities in Solove's taxonomy. Neither the PolG NRW nor the KPL display awareness that processes of (1) data processing and (2) data distribution have to be identified as privacy risks as well. Only acts of information gathering have limitations placed upon them. Neither data aggregation, secondary use, storing nor increased accessibility are recognised as harmful activities. This is also reflected in the KPL. As it has been established privacy protection limits itself within the KPL to the act of information gathering. This limitations does *not* allow to consider processes that follow data gathering to be considered as potentially harmful activities. The analysis has shown that § 22, 22a, 23, 24, 26, 27 all enable and facilitate information gathering, information processing and distribution activities that must be recognised to infringe upon privacy**.** The only protection in place against activities in these clusters are deleting obligations, which only scratch the surface of harmful activities within processing and distribution that can be harmful to the data subject. Privacy protection both the PolG NRW and the KPL only consider information collection to be harmful. And even within information collection, formulations remain vague, regulatory systems to control surveillance practices render themselves obsolete in case of § 20c.

Second, the PolG NRW infringes upon personal privacy through § 20c. As per my analysis, the permission to conduct telecommunication surveillance of messenger services is hardly defendable. The only protection in place, the Kernbereich privater Lebensgestaltung, is easily avoided. Legally, an investigator must determine beforehand whether he or she will infringe upon privacy. However, the very content that comes out of the telecommunication surveillance will determine whether the surveillance was permissible. At this point, the police will have already harmed privacy rights of a potentially innocent citizen. While any data would be deleted if the data subject turns out to be innocent, the privacy of the data subject has been breached without notice to the data subject. To be fair, § 20c does have limitations in place to protect dignity and the KPL of the individual. However, as previous sections already illustrated the focus of privacy protection in both § 20c and the KPL is flawed. Rather than focusing on protecting secrecy, as seen in the emphasis on Kernberreich, a law that potentially enables

infringements upon privacy *must* anticipate practical and applicable harms and problems caused by surveillance. Merely referring to a private sphere that shall remain untouched by state interference, formulates privacy concerns in such an abstract way that it becomes increasingly harder to define and apply to cases. Additionally, all paragraphs of the PolG NRW that were reviewed so far, fail to allow the data subject to know about the data that others have about him or her and its handling and use. By EU Law, right of access and correction concerning collected data must be provided (Solove, 2010). If the data subject is left in the dark about the records maintained about him or her by government agencies and businesses, the data subject grows increasingly vulnerable and uncertain.

Third, in light of the uncomplete understanding of privacy, data is stored for an alarmingly long time without scrutiny. The 'Bundestag Hack' exemplifies that no network is completely safe. Anonymisation measurements would do little to combat this. However, the Police does not even need to anonymise data that is shared online, across precincts and across county state borders within Germany.

## 6.3 Conclusion and Final Thoughts

No research has been conducted yet that discusses surveillance policy the privacy taxonomy as well as conceptual analysis. Future research might improve through the usage of both a taxonomy of privacy and conceptual analysis in surveillance and policing policy. First, the taxonomy of privacy allows to identify activities, rather than focusing the discussion on abstract and vague interests of why privacy is worth protecting. Second, working about the perception of privacy allows to identify the root of problematic surveillance practices. This allows to work out better suggestions and more applied accounts on (1) what is worth improving and (2) why it is worth improving.

In this thesis, I have demonstrated how the elusive nature of the concept of privacy is at root of why discussion surrounding infringements upon privacy has proven to be tedious and not well articulated. Surveillance practices now available to the police, enabled through the newly revised PolG NRW, pose an alarming threat to privacy. The privacy taxonomy by Solove (2010) allowed me to shed light on the fact that the conception of privacy reflected both in the (1) PolG NRW as well as (2) the KPL map a rather singular perception of privacy. Since the revised PolG NRW was implemented by December 2018, practices of policing following this new law are not yet known. Often times, there is a gap between law and practice. On a theoretical side, however, the introduced changes pose an alarming threat to privacy.

Throughout this analysis it became apparent that privacy is seen at risk, *only* when people are being surveilled. This is formerly recognised throughout the Kernebereich and PolG NRW. As per the previous analysis, privacy can be harmed through activities that follow the data collection process. The storing, combining, aggregating, and second using of data bears a risk. These processes are not legally recognised to pose a threat to privacy in Germany. This comes as no surprise. If the very basis for privacy protection in Germany, the KPL, does not consider anything beyond the act of watching and listening to harm privacy rights, no new regulation will start to consider more wide-reaching and abstract activities that harm privacy. Any surveillance policy and practice is limited by the KPL both in a positive as well as in a negative sense. Considerations taken to protect the data subject from surveillance work in so far as that they put strict regulations on how data can be acquired. However, anything beyond is not considered. Disregarding important processes of data handling that follow the act of surveillance itself puts the individual at serious risk. Hence, present and future policy must employ a

more thoroughly developed understanding of privacy in order to anticipate currently and previously disregarded harmful activities.

## Reference List


Amnesty International. (2018). Neuer Entwurf zum Polizeigesetz in NRW: Gute Ansätze, noch mehr Versäumnisse. Retrieved June 8, 2019, from https://www.amnesty.de/informieren/aktuell/deutschland-neuer-entwurf-zum-polizeigesetz-nrw-gute-ansaetze-noch-mehr

Bronk, C (2008). Hacking the Nation State: Security, Information Technology and Policies of Assurance [Abstract]. Information Security Journal: A Global Perspective. Vol. 17, No. 3. doi: 10.1080/19393550802178556 5

de Bruin, B. (2010) The liberal value of privacy. *Law and Philosophy*, Vol. 29, No. 5, pp. 505–534.

Gavison, Ruth E. (2012). Privacy and the Limits of Law (May 16, 2012). *The Yale Law Journal*, Vol. 89, No. 3, pp. 421-471. Retrieved from https://ssrn.com/abstract=2060957

Germany, German Ministry for Political Education, BPD. (n.d.). *Persöhnlichkeitsrecht.* Berlin.

Germany, Polizeigesetz des Landes Nordrhein-Westfalen, Landtag NRW (2019).

Gusy, C., Dr. (2018). Stellungnahme zum Gesetzentwurf 6. Änderungsgesetz des PolG NRW. Universität Bielefeld, Bielefeld. Retrieved from: https://www.landtag.nrw.de/Dokumentenservice/portal/WWW/dokumentenarchiv/Dokument/MMST17-630.pdf

Götschenberg, M. (2019). Hacker veröffentlichen persönliche Daten von Politikern. *Deutschlandfunk*. Retrieved June 8, 2019, from https://www.deutschlandfunk.de/cyberangriff-auf-bundestag-hacker-veroeffentlichen.1773.de.html?dram:article_id=437443

Habermas, J. (1987). The theory of communicative action (Vol. 2.). Boston, MA: Beacon Press.

Himma, KE (2007) Privacy versus security: why privacy is not an absolute value or right. *San Diego Law Review.* Vol. 44, No. 4, pp. 859–919

Landynski, J.W. Privacy, Law, and Public Policy. David M. O'Brien: *The Journal of Politics*. Vol. 43, No. 2, pp. 594-596.

Lever, A (2013). A Democratic Conception of Privacy. Bloomington: AuthorHouse.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society.* Vol. 1, No. 2. doi:10.1177/2053951714541861

Lyon, D. (2001). Surveillance after September 11, 2001. *The Intensification of Surveillance,* Vol. 6, No. 3, pp. 16-25. doi:10.2307/j.ctt18fs7k5.5

Marmor, A (2015) What is the right to privacy? *Philosophy & Public Affairs.* Vol. 43, No. 1, pp. 3-26.

Papathanassopoulos, S. (2015). Privacy 2.0. *Social Media Society.* Vol. 1, No.1. doi:10.1177/2056305115578141

Polizei Gewerkschaft Deutschland [Police Labour Union Germany]. (2018, May 30). *Stellungnahme: Gesetz zur Stärkung der Sicherheit in Nordrhein-Westfalen*[Press release]. Retrieved April 15, 2019.

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

Schnell, L. (2018). Bayern hat das schärfste Polizeigesetz in Deutschland. *Süddeutsche Zeitung*. Retrieved June 8, 2019, from https://www.sueddeutsche.de/bayern/polizeiaufgabengesetz-inhalt-bayern-1.3973927

Sen, A. (1982). Rights and Agency. *Philosophy & Public Affairs.* Vol. 11, No. 1, pp. 3-39. Retrieved April 15, 2019, from https://www.jstor.org/stable/2265041.

Solove, D. J. (2010). Understanding privacy. Cambridge, MA: Harvard University Press.

Taylor, I. (2017). Data collection, counterterrorism and the right to privacy. *Politics, Philosophy & Economics.* Vol. 16, No. 3, pp. 326-346. doi:10.1177/1470594x17715249

Teigeler, M. (2018, December 6). Polizeigesetz: Grüne drohen mit Verfassungsklage. *WDR*. Retrieved June 8, 2019, from https://www1.wdr.de/nachrichten/landespolitik/polizeigesetz-gruene-100.html

Thompson, J. J. (1975). The Right to Privacy. *Philosophy & Public Affairs.* Vol. 4, pp. 295-314. Retrieved April 15, 2019, from https://www.jstor.org/stable/2265075?seq=1#metadata_info_tab_contents.

Turnage, A.K. (2007) Surveillance and Security: Technological Politics and Power in Everyday Life by Monahan, T. *The Communication Review*. Vol. 10, No. 4, pp. 391-396. doi:10.1080/10714420701715514

Van Lieshout, M., Friedewald, M., Wright, D., & Gutwirth, S. (2012). Reconciling privacy and security. *Innovation: The European Journal of Social Science Research.* Vol .26, No. 1-2, pp. 119-132 doi:10.1080/13511610.2013.723378

Walzer, M (2015) Just and Unjust Wars: A Moral Argument with Historical Illustrations (5th edition). New York: Basic Books.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review.* Vol. 4, No. 5, p. 193. doi:10.2307/1321160

Zimmer, M. (2010). ''But the data is already public'': On the ethics of research in Facebook. *Ethics in Technology.* Vol. 12, pp. 313-325. doi:10.1007/s10676-010-9227-5

Figures:

*Figure 1*. A taxonomy of privacy. Adapted from 'Understanding Privacy', by Solove, 2010, Cambridge MA: Harvard University Press.