ANOUK MOLS

EVERYDAY EXPERIENCES OF PRIVACY AND SURVEILLANCE

NEGOTIATING APPROPRIATE FORMS OF MONITORING

Everyday experiences of privacy and surveillance

Negotiating appropriate forms of monitoring

This dissertation is part of the *Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems* project which is financed by the Netherlands Organisation for Scientific Research (NWO) under the Privacy Research in Cyber Environment (PRICE) grant, number: 628.001.024

ISBN: 978-90-76665-47-4
Publisher: Erasmus Research Centre for Media, Communication and Culture
Series: ERMeCC Doctoral Dissertations, nr. 27
Printed by: Ipskamp Printing
Cover design and illustrations: Jeroen Mols (www.jeroenmols.nl)

Everyday experiences of privacy and surveillance

Negotiating appropriate forms of monitoring

Alledaagse ervaringen met privacy en surveillance

Gepaste vormen van monitoring overwegen

Thesis

to obtain the degree of Doctor from the
Erasmus University Rotterdam
by command of the
rector magnificus

Prof.dr. A.L. Bredenoord

and in accordance with the decision of the Doctorate Board.
The public defence shall be held on

Wednesday 8 December 2021 at 13.00hrs
by

Anouk Evelien Mols
born in Naarden, the Netherlands.

Erasmus University Rotterdam

Doctoral Committee

Promotor:	prof.dr. M.S.S.E. Janssen
Other members:	prof. dr. C.L. ter Hoeven
	prof. dr. V. M. Steeves
	dr. D. Trottier
Copromotor:	dr. J.H. Pridmore

This one is for my boys

Acknowledgments

Welcome to the world, dissertation. You would never have been here if it wasn't for all the fantastic people that were part of your development. I would like to thank all of them. I'm grateful to all the respondents for sharing their experiences with me. And to my supervisors: Susanne, thank you for your support throughout the years. Jason, thank you for your trust in me and for making this project a light-hearted endeavor. I'm looking forward to working with you for a couple more years!

Many people in the M&C department and ESHCC faculty made this PhD journey worthwhile: To the best office mates: Shangwei, let's keep in touch and Tessa, let's rock our next project. Evelien, thank you for cheering me on. Daniel, I enjoyed spending time with you at airports. Qian, you're an amazing cook. Yijing, Anne, Aleid, Rashid, Ana, Tonny, Palesa, Joao, Jorge, Selma, Bartosz, Renee, Apoorva, Karen, Carmen, Arne, Massimo, Hoan, Siri, Arno, Qiong, and many others, thank you for being great colleagues!

Part of this dissertation is about the blurring of boundaries. Rian, Simone, and Yosha, our WhatsApp chat is the true embodiment of blurring boundaries between work and personal life. I hope we will never stop sharing our loeder-moedermoments and work experiences.

When it comes to life outside of this PhD, I want to thank all my friends for being great company, distraction, and fun. Thank you Denise and Mirte, Jelmer and Simone, Vanessa, Yvonne, Eva, Willeke, Christine, Nathalie, Tessa, de Valeriootjes, and Brigitte, Leanne and the other travel troopers. I'm also incredibly grateful for all the support I've received from my family, Annette (mam) and Joost (pap) and Paulien and Ruud, thank you for being there for us and for being interested in my PhD throughout the years. To my oma Corrie, my (bonus) siblings Yannick, Sara and Bauke, Mirthe and Fred, my amazing nieces Mila, Feline, and Thirza, and awesome nephew Abe, I love spending time with all of you. And to my uncle Jeroen, thank you for the wonderful cover design and illustrations.

As stated on the previous page: *this one is for my boys*. Jim, I know it is a cliché but I honestly couldn't have done this without your endless support, love, and care. I love you. Jonas and Mats (aka kletskous and klauterkees), the best thing about life is being your mother. Your giggles, cuddles, and kisses make every day a good day.

Table of contents

Appendices

Summaries

Chapter 1

Introduction Everyday privacy and surveillance experiences

I don't care about privacy.

This statement could be true if you inventory my everyday practices: I regularly shop online, have a Gmail account and a Twitter profile, only occasionally block cookies, consult Google Assistant at times, use banking apps often, and have a digital Covid-19 vaccination certificate on my smartphone. Moreover, my data doubles – flows of my data collected via digital surveillance and aggregated into various profiles (Haggerty & Ericson, 2000; Lyon, 2018) – also indicate that I do not care about privacy. Yet, if you would ask me, I would tell you that privacy matters to me and that I often try to limit the impact of surveillance on my life. Whereas the chasm between my behaviour and attitude might be considered a so-called privacy paradox (Barnes, 2006; Brown, 2001), this concept does not account for all the small-scale considerations around surveillance and privacy I take on a daily basis.

Rather than my behaviour being paradoxical or centred around a privacy calculus (Bol, Dienlin, et al., 2018; Dinev & Hart, 2006), my experiences are multidimensional and situated within the things I do and say on a daily basis. This is visible in a brief overview of some of my practices: To limit digital lateral, or peer-to-peer, surveillance (Andrejevic, 2002), I disabled WhatsApp's *last seen* features so that my contacts cannot check the last time I opened the app. To avoid lateral surveillance in the physical sense, I close my curtains at night to prevent neighbours from peeking in. To limit commercial consumer surveillance (Pridmore & Zwick, 2011), I only use Google Assistant on occasion in my car and switch it off in other places. To manage the boundaries between work and personal contexts (Nippert-Eng, 1996b), I often leave my laptop in my study. Finally, considerations around the intimate surveillance of my children (Leaver, 2017) are visible in how I regularly check pictures shared by their day-care via a mobile application but also put up informational boundaries (Petronio, 2010) by restricting anyone from posting pictures of my two sons on social media.

These examples show that I essentially care about privacy. My everyday experiences of privacy and surveillance entail flexible practices which are integrated in constellations of other practices. These experiences are situated in particular (often overlapping) contexts like my family life, work environment, neighbourhood, and social connections. Privacy and surveillance are two intangible concepts only experienced directly when privacy breaches take place and/or when we are confronted with specific surveillance incidences. This makes it difficult for most people to explain what these concepts mean to them. Furthermore, my personal examples show that what I do offers a richer and more complete account of how I experience privacy and surveillance than what I say. In this dissertation, I aim to better understand experiences of privacy and surveillance, and particularly how people experience these intangible concepts in their everyday lives. Therefore, the overarching research question is:

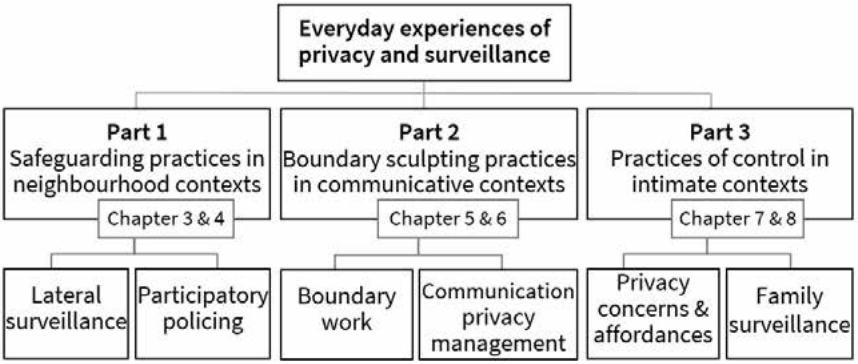
> **How do people experience privacy and surveillance in their everyday practices?**

Exploring this question through an in-depth, qualitative account of sociomaterial practices in different contexts allows me to contribute to existing research in the field of privacy and surveillance. Privacy and surveillance practices are inherently sociomaterial because they entail interactions between people, devices, and (digital) technologies (more on this in Chapter 2). Based on the research findings, I offer practical advice for individuals, educators, and parents to increase privacy and surveillance awareness and resilience. To understand how people deal with surveillance and privacy in their everyday lives, this dissertation focuses on three contexts where such experiences take place; safeguarding practices in community contexts, boundary sculpting practices in communicative contexts, and practices of control in intimate contexts (see Figure 1). In this introductory chapter, I first describe these different contexts and the technologies that are intertwined with everyday privacy and surveillance practices. Afterwards, privacy and surveillance are presented as the core theoretical concepts of this research, followed by insights into the Dutch research setting and a brief outline of the dissertation.

Three contexts of privacy and surveillance experiences

This dissertation includes three empirical parts, each existing of two chapters focusing on privacy and surveillance experiences in the contexts of safety, boundaries, and control. Figure 1 indicates how these contexts form the basis of six empirical studies exploring practices through the lens of specific theories and concepts. More specifically, Part 1 explores neighbourhood watchfulness practices with a focus on lateral surveillance (Chapter 3) and participatory policing (Chapter 4). Part 2 approaches communication practices a form of boundary work (Chapter 5) and communication privacy management (Chapter 6). Finally, Part 3 discusses how the home as an intimate context of control provides the backdrop for privacy concerns about the affordances of smart speakers (Chapter 7) and for family surveillance practices (Chapter 8). Below, I discuss why these three contexts are crucial areas for studying everyday privacy and surveillance experiences.

Figure 1: Overview of research contexts and concepts



Everyday experiences of privacy and surveillance

Part 1 Safeguarding practices in neighbourhood contexts — Chapter 3 & 4: Lateral surveillance; Participatory policing

Part 2 Boundary sculpting practices in communicative contexts — Chapter 5 & 6: Boundary work; Communication privacy management

Part 3 Practices of control in intimate contexts — Chapter 7 & 8: Privacy concerns & affordances; Family surveillance

Part 1: Safeguarding practices in community contexts

The first empirical part of my dissertation focuses on interconnected citizens who safeguard their neighbourhood via WhatsApp neighbourhood crime prevention (WNCP) groups, a popular phenomenon in the Netherlands. In Chapters 3 and 4, I present the results from interviews and focus groups with moderators and members of such groups. Since 2013, more than 9,000 WNCP groups have been registered online[1] and the popularity of WNCP groups can be explained by their low participation threshold and easy accessibility (Bervoets et al., 2016). This is mainly induced by the user-friendly and convenient nature of WhatsApp, a smartphone messaging application with a high penetration rate in the Netherlands – as of 2021, 82% of the Dutch population of 15 years and older uses WhatsApp (Van der Veer et al., 2021).

Through the use of WhatsApp, groups of neighbours exchange warnings, concerns, and information about incidents, emergencies and (allegedly) suspicious situations related to their community. These exchanges often lead to citizens actively protecting and monitoring their streets, using camera-phones to record events or people they deem suspicious. WNCP groups are a fascinating context for studying privacy and surveillance practices because they enable an examination of how community initiatives around safety have a direct impact on the neighbourhood dynamics and personal experiences of citizens. The fact that these WNCP groups have become such a wide-spread phenomenon in the Netherlands in less than a decade indicates that this is a phenomenon that is partly normalised but that citizens are at the same time still working out ways to deal with the presence of WNCP in their daily lives.

Existing research shows that WNCP practices have ambivalent personal and community consequences. According to Akkermans and Vollaard (2015), the introduction of WNCP to neighbourhoods in Tilburg considerably decreased the number of break-ins. Their study measured break-in rates before and after the introduction of WNCP and neighbourhood block watch groups. While these findings are often repeated by

[1] People can register their WNCP group on the website https://wapb.nl which enables citizens to find and connect to groups in their neighbourhood. It is suspected that the actual number of active WNCP groups in the Netherlands is much higher because not all groups are registered.

news media, the question remains whether WNCP groups actually decrease property crime or displace it to surrounding neighbourhoods. WNCP groups in Tilburg might have instigated a *water bed effect*, i.e. a temporary relocation of criminality or break-ins to other neighbourhoods (Van der Land et al., 2014). While the main purpose of WNCP groups is to prevent break-ins, increased social cohesion is also mentioned as a positive effect (Mehlbaum & Steden, 2018; Van der Land et al., 2014). Moreover, some participants feel good about being aware of activity in their neighbourhood, or feel safer when they know about neighbourhood safeguarding practices (Smeets et al., 2019).

In contrast, an increased anxiety about safety can also be caused by WNCP group participation (Lub & De Leeuw, 2017). Apart from these personal drawbacks, the neighbourhood culture can be affected by stereotyping, racist behaviour, and privacy-infringing practices (De Vries, 2016; Lub & De Leeuw, 2019). Building on these reports and studies, Part 1 provides a deeper level of understanding of neighbourhood watchfulness practices and experiences. Chapter 3 highlights how sociomaterial dimensions of WNCP practices can be seen as a form of lateral surveillance (Andrejevic, 2002) and Chapter 4 presents an in-depth account of how WNCP moderators and participants experience privacy and surveillance in precarious participatory policing efforts (Larsson, 2017; Reeves, 2012).

Part 2: Boundary sculpting practices in communicative contexts

Communicative contexts form the second empirical part of this dissertation. In Chapters 5 and 6, digital interactions form the backdrop for boundary sculpting practices around absence and presence, personal information, and between different relational contexts. The main communicative context in Part 2 is the messaging application WhatsApp. Since its introduction in 2009, WhatsApp allows individuals to send and receive images, video, audio, and location-based messages in one-to-one, one-to-many, or group conversations (Seufert et al., 2016). As mentioned before, WhatsApp is widely used in the Netherlands. WhatsApp is a cross-platform smartphone-based messaging application and its private nature and end-to-end encryption made the application popular for personal conversations (Church & de Oliveira, 2013; Karapanos et al., 2016). By default, WhatsApp makes no distinction between different contexts—all conversations are accessible in the same location causing digital contexts to collapse (Marwick & boyd, 2010; Vitak et al., 2012). Like most messaging apps, WhatsApp provides additional information, such as message delivery notifications (in the form of *blue checks*), when individuals are online, when they are typing, and when they last accessed the application (the *last seen* setting) (Church & de Oliveira, 2013).

While WhatsApp provides the most often used digital communication platform for the respondents in Chapters 5 and 6, other messaging apps (like Signal and Facebook Messenger) and social media are also discussed as additional or alternative communication channels. Moreover, some respondents also use communication platforms designated for work such as enterprise social media, Slack, and email. What makes communicative contexts such a crucial area of study is that digital interactions have become an integral part of everyday practices. Most people engage in various digital conversations via WhatsApp and other platforms throughout the day. This makes them automatically subject to lateral surveillance by their social contacts and commercial surveillance by digital platforms. Privacy protection efforts around digital communication are constrained by social expectations that urge people to be continuously present, available, and responsive. The interview-based research in Part 2 adds to existing research about digital communication practices (Burchell, 2015; Seufert et al., 2016) by showing that social influences make privacy and surveillance experiences in communicative contexts ambivalent and multidimensional.

In Chapter 5, I show how particular features of smartphones and messaging apps play a role in how individuals experience privacy. Respondents manage absence and presence with the help of WhatsApp functions and sculpt digital boundaries between different relational contexts including work, private life, and neighbourhoods. This chapter builds on research about physical/digital context collapse (Pagh, 2020), negotiated networked absence (Burchell, 2017), and boundary theory (Nippert-Eng, 1996a). Chapter 6 has a narrower focus on digital workplace communication and shows how personal information disclosure and protection practices pose specific challenges for different professional groups. I present communication privacy management (CPM) as a way that Dutch managers, office employees, self-employed professionals, and service industry employees manage boundaries around private information disclosure (Petronio, 2012). Their digital workplace communication can be characterised as dispersed because it takes place via multiple devices and various platforms. The respondents carefully establish privacy rules to manage the boundaries around the disclosure and protection of information.

Part 3: Practices of control in intimate contexts

The third empirical section of my dissertation presents homes (Chapter 7) and families (Chapter 8) as intimate contexts where practices of control take place. Chapter 7 presents the results of a survey and focus groups with university personnel about privacy concerns around household Intelligent Personal Assistants (IPAs). Household IPAs, also known as smart speakers, can be used to control the home environment and were directly preceded by IPAs on smartphones. Such voice activated virtual assistants include Apple's Siri, Google Assistant/Google Now, Microsoft's Cortana, and Samsung's Bixby. While phone IPAs function via an app and are not bound to a location, household IPAs work with the same technology but take the form of standalone devices which need an Internet connection and power to function. IPAs can be activated with a trigger word in order to set alarms or timers, stream music or videos, control smart appliances (such as lamps, smart TVs, and door bells), listen to news bulletins or weather forecasts, call someone, access calendars, send text messages, or make purchases (Kinsella & Mutchler, 2019).

The survey and focus groups were conducted shortly before household IPAs were introduced to the Dutch market and explored the initial privacy concerns of potential users. Whereas some respondents perceived the benefits of controlling their house via a smart speaker, most also voiced multidimensional privacy concerns around surveillance, security, and platforms that were instigated by particular affordances, or possibilities for action (Evans et al., 2017). Chapter 7 presents an affordance-focused and multidimensional account of privacy concerns and adds to a growing body of research about smart technologies and privacy perceptions (Huang et al., 2020; Liao et al., 2019; Manikonda et al., 2017).

Finally, Chapter 8 takes place in intimate family contexts and revolves around family surveillance. Family surveillance can be defined as keeping track of family members' digital and non-digital activities and associations. This research is based on interviews with parents and children and explores their media repertoires and family surveillance practices. Parents are concerned about the technology use of their children and often engage in restricting and monitoring practices of screen time, social media, and smartphones (Livingstone, Mascheroni, Dreier, et al., 2015; Marsh et al., 2017; Marx & Steeves, 2010). Dutch parents sometimes engage in digital parental monitoring of (early) adolescents' locations via location tracking apps, use student tracking systems to keep an eye on education progress, and check their children's social media use. Their children actively respond to family surveillance practices. Chapter 8 provides an account of family surveillance contextualised by family histories, media repertoires, and interactions which is inspired by the work of Ervasti et al. (2016), Jeffery (2021), Livingstone (2014), Mazmanian and Lanette (2017), and Steeves et al. (2020).

Research foundations: Privacy and surveillance

After having established this dissertation's three research contexts, I now present privacy and surveillance as the core theoretical foundations. It is important to note that surveillance is intrinsically connected with privacy, yet they are not opposites. Rather than surveillance being the *bad* and privacy the *good* side of the coin, both can be good for individuals and for society yet can also have negative consequences (Marx, 2015a). This section presents an outline of (some of) the seminal works in the field of privacy and surveillance. Furthermore, the six empirical chapters are informed by particular theoretical angles and I highlight how my studies build on and add to existing research in the field of privacy and surveillance.

Introducing privacy as a multidimensional concept

Privacy is a fluid and abstract concept, loaded with moral considerations and views about rights, personal values, human freedom, and information flows. There are many definitions of privacy connected to different aspects of human life and the concept is often seen as essentially contested due to its openness and internal complexity (Mulligan et al., 2016). A far from conclusive list of influential conceptualisations of privacy includes: early notions of privacy emphasising a *right to be let alone* (Warren & Brandeis, 1890); privacy as controlling *access to (information of) the self* (Westin, 1967); privacy as *boundary negotiations between openness and closedness* (Altman, 1975); a philosophical focus on controlling access to one's inner aspects whereby privacy is related to *intimacy*, *trust*, and *identity* (Schoeman, 1984); legal perceptions of privacy as *control-over-information* and *personal information as property* (Solove, 2002); critical political notions of privacy addressing *unequal divisions of power and data ownership* (Allmer, 2013; Fuchs, 2012); and a socially oriented view of privacy as *a common good* or *collective value* (Regan, 2015; Solove, 2008).

This dissertation follows the latter conceptualisation and approaches privacy as **a social and multidimensional concept which is enacted through physical and digital boundaries**. Before describing a social notion of privacy in more detail, I present Koops et al.'s typology of privacy (2016) as a helpful approach to grasp the multidimensional nature of privacy. Their typology exists of nine types of privacy that people restrict, control, or limit access to. The first is *information* privacy which can be seen as integral to as well as overarching other types. The other eight types concern the physical body (*bodily* privacy), private spaces such as homes (*spatial* privacy), mediated and unmediated communication (*communicational* privacy), items or information shielded by property (*proprietary* privacy), thoughts and minds and the development of opinions and beliefs (*intellectual* privacy), decision-making in intimate contexts (*decisional* privacy), choices of who to interact with (*associational* privacy), and activities in public (*behavioural* privacy) (Koops et al., 2016). This typology provides much needed insights into how privacy can be experienced differently in relation to particular objects, contexts, and practices. I apply this typology in Chapter 7 which shows that privacy concerns around household IPAs specifically relate to some of Koops et al.'s (2016) types of privacy. This dissertation also builds on social approaches to privacy which are presented below.

Social privacy, contextual integrity, and boundary management

Most seminal views on privacy focus on individualistic rights from a legal or philosophical perspective and overlook the importance of privacy for democratic societies in supporting social interactions (Hughes, 2015). Regan (2015) focuses on the social aspects of privacy and presents it as a social value in order to reflect its common importance for all people, the increase of public and political surveillance, and the interconnected nature of privacy. Steeves (2009) goes beyond an information-focused notion of privacy and turns to the social context because privacy is socially constructed and negotiated in social relationships. Moreover, Steeves (2015) argues that a social notion of privacy should form the basis of privacy legislation because privacy plays a crucial role in developing social relationships and identity (especially for children). Privacy also facilitates social interactions and in order to understand privacy, *"we need to examine the ways in which privacy is experienced" (*Hughes, 2015, p. 230). Several researchers provide helpful frameworks for socially oriented examinations of privacy, three of which are important for the research in this dissertation.

Privacy as contextual integrity

Nissenbaum (2004, 2010, 2019) focuses on the social value of privacy in different contexts. The concept of privacy as contextual integrity revolves around appropriate flows of information. This framework focuses on *informational norms* of appropriateness which are shaped by four parameters: First, *contexts* are structured differentiated spheres in social life such as family homes where parent-child interactions take place (e.g., as discussed in Chapter 8). Second, *actors* concern the senders and recipients of information and information subjects (all of which can be single or multiple individuals or collectives) – to illustrate, Chapter 6 addresses managers as actors in workplace communication. Third, *attributes* or information types describe the nature of the information in question. For example, Chapters 3 and 4 show that neighbours in WNCP groups share the character traits, location, and activities of allegedly suspicious persons. Finally, *transmission principles* constrain the flows of information. For instance, household IPA platforms (such as Google, Amazon, and Apple) can only process information when the user provides consent (Chapter 7).

It is important to note that such smart devices entail data aggregation practices which provide challenges to contextual integrity because they mainly take place under the radar of privacy norms (Nissenbaum, 2019). In sum, privacy expectations are embodied in norms about information flows determined by the context, involved actors, nature of information, and terms and conditions (Nissenbaum, 2010). Because privacy as contextual integrity mainly focuses on informational privacy while my research approaches privacy as a multidimensional experience, this theory is not directly applied in the empirical chapters. Yet, in the concluding Chapter 9, privacy as contextual integrity informs the answer to the main research question. Moreover, my research provides some insights into how (physical/digital) context collapse complicates privacy as contextual integrity.

Informational boundaries: Communication privacy management (CPM)

Whereas privacy as contextual integrity explains how privacy norms take form and how appropriate information flows are established, communication privacy management (CPM) theory focuses on how individuals (the *actors* as senders and subjects) actively manage information they consider private (Petronio & Child, 2020). This happens continuously via flexible metaphorical boundaries which regulate and control the disclosure and concealing of private information (Petronio, 2010, 2012). Thick boundaries might be installed to offer a high level of control and many restrictions to access when an employee wants to conceal their religious beliefs in their workplace. Thin and more permeable boundaries providing only moderate control might suffice for regulating access to less sensitive information like an employee's holiday destination. The core general concepts of CPM, *ownership, privacy rules,* and *turbulence*, are explained in Chapter 6 of this dissertation where I also describe how information privacy rules and boundaries form tangible aspects in everyday (digital) workplace communication. Chapter 6 adds to existing CPM research (Frampton & Child, 2013; Krouse & Afifi, 2007; Laitinen & Sivunen, 2020; Petronio, 2002; Smith & Brunner, 2017; Snyder & Cistulli, 2020) with a sociomaterial account of how CPM practices differ across professional roles and communication platforms.

Interpersonal boundaries: Boundary theory

Privacy as contextual integrity and communication privacy management theory are both helpful in understanding how individuals perceive and manage flows of information. However, in order to fully understand privacy as a social construct, it is important to move the focus from information flows to social interactions (Steeves, 2009). The work of Nippert-Eng (1996a, 1996b, 2010) provides tools to investigate social interactions in relation to privacy. Nippert-Eng (2010) views privacy through the lens of mundane social practices, and explores how people manage the boundaries between privacy and publicity, accessibility and inaccessibility, and concealment and disclosure. Privacy is experienced in a way that goes beyond controlling access to information flows as it also entails the freedom of being alone and making unrestricted decisions. Privacy experiences are based on a managerial elements and constant negotiations (Nippert-Eng, 2010).

Chapter 5 describes Nippert-Eng's (1996a, 1996b) earlier work on boundary theory which explains how people manage socio-cognitive borders between work and home contexts. Such boundaries offer individuals the means to (partly) integrate or segment these different contexts, and are often tangible when enacted via objects, activities, and tasks. The study in Chapter 5 adds to research about boundary theory (Jahn et al., 2016; Siegert & Löwstedt, 2019) by presenting sociomaterial boundary sculpting practices across different relational contexts such as family life, workplace, and neighbourhood.

Social privacy can be experienced or invaded in the physical sense (e.g., when a neighbour peeks through a window) as well as in the digital sense (e.g., when a picture is forwarded to others without consent of the sender). This reinforces that we should not separate the physical from the digital in studying privacy, because these are intrinsically connected (Koops, 2018). Physical and digital contexts are not only interconnected but also collapse often because digital media allow for individuals to *"perform practices in a wider array of spatial and temporal settings"* (Pagh, 2020, p. 2811). For instance, people can attend an online funeral while getting a haircut at their beauty salon (this anecdote was shared by my hairdresser and provides a real-life example of being present in a physical and digital environment simultaneously). Needless to say, context collapse also informs this research that covers multiple contexts. Throughout this dissertation, I follow Nippert-Eng's (2010) example of studying mundane attempts of *doing* privacy. I also provide insights into how individuals *do* surveillance by monitoring their neighbourhood, colleagues, and family members. The next section provides an overview of surveillance as the other key concept of this dissertation.

Multidimensional surveillance practices

Similar to privacy, surveillance is a multidimensional concept. Lyon (2018, p. 12) defines surveillance as *"the operations and experiences of gathering and analysing personal data for influence, entitlement and management".* Surveillance entails an *"agent who accesses (whether through discovery tools, rules or physical/logistical settings) personal data"* (Marx, 2015a, p. 33). In other words, surveillance exists of personal data collection and processing practices of a great variety of actors for an even greater number of reasons. Surveillance it is not directed by *"one centralised entity, but is polycentric and networked"* (Niculescu Dinca, 2016, p. 62). This has to do with the multiplicity of (interconnected) surveilling actors and with the diversity of data flows collected via different channels. Also, personal data (collected for commercial use, government purposes, or police investigations) can be endlessly recombined and re-used and different types of surveillance data obtained in different sectors or contexts can potentially be used for cross-referencing and linking (Lyon, 2007). Surveillance can be understood as a *surveillant assemblage* which comprises the convergence and assembling of different data flows (Haggerty & Ericson, 2000). Ubiquitous mobile and interconnected technologies and devices increase the potential for pervasive forms of digitally mediated surveillance. In fact, people's day-to-day life can be seen as being under constant surveillance, because people are immersed in networked technologies throughout the day and on all locations (Lyon, 2007):

> *"Surveillance is an everyday fact of life that we not only encounter from outside, as it were, but also in which we engage, from within, in many contexts… Today, much surveillance is still a specialised activity, carried out by police and intelligence*

> *agencies and, of course, by corporations. But it is also something that is done domestically, in everyday life…Watching has become a way of life."*
> (Lyon, 2018, p. 11)

These definitions of surveillance highlight its multidimensional nature. In this section, I explain how surveillance for policing, commercial, and interpersonal purposes is embedded in the empirical research in this dissertation.

Surveillance and policing

Policing practices are intertwined with surveillance practices because an important part of crime control revolves around collecting information. Particularly, policing takes place in an institutional matrix and *"the police increasingly rely on forms of monitoring that are conducted by other government, security and commercial actors"* (Haggerty, 2012, p. 236). This quote indicates how monitoring practices and forms of data collection and processing by different actors for various purposes intertwine. This often entails surveillance creep; when surveillance measures intended for one purpose are used for additional or alternative purposes (Haggerty, 2012). Police actors engage in various forms of surveillance, among which undercover policing, making use of secondary information (e.g., via informants), using surveillance technologies such as satellites, helicopters, drones, sensors, camera's, and biometric and DNA databases, and collecting and processing online (big) data – also described as *dataveillance* (Haggerty, 2012).

Another form of police surveillance can occur in interaction with citizens when these engage in participatory policing practices such as monitoring, sharing information, reporting suspicious behaviour or threats, and actively preventing crime (Larsson, 2017). Participatory policing is often initiated in a top-down manner, either via nationwide public vigilance campaigns wherein law enforcement asks citizens to be alert towards particular (signs of) threats and criminal or terrorist activity and to share information (Larsen & Piché, 2010; Larsson, 2017; Reeves, 2012), or through local projects and campaigns with community police-led participatory policing practices (Ryan, 2008; Shearing, 1994;

Varghese, 2009; Walker & Walker, 1990). Such forms of citizen surveillance require a vigilant mindset. Citizens keep an eye out for suspicious or dangerous behaviour, events, and persons – processes that normalise distrust (Larsson, 2017). This dissertation includes research on citizen-initiated surveillance practices of citizens. To be more precise, Chapter 4 highlights how voluntary lateral surveillance in WNCP groups forms the basis of participatory policing practices. By providing an in-depth account of the problematic consequences of citizens' self-responsibilisation, I add to existing research about participatory policing.

Consumer surveillance, platforms, and surveillance capitalism

Another form of surveillance is targeting consumers and is intimately connected with marketing (Pridmore & Zwick, 2011). Companies can use a plethora of *consumer surveillance* technologies fuelled by consumer data, like *"targeted advertisements, web site 'cookies', tailored promotional materials, differing levels and promptness in customer service, social media feedback channels, viral marketing, diverse or tiered pricing structures, and others"* (Pridmore, 2012, p. 321).The surveillance of consumers has become more seamless, interconnected, and comprehensive over the years. Databases are used to create long-term profitable relations with consumers as well as to segment and target them. Whereas all respondents are using interconnected technologies and are consequently subjected to consumer surveillance, this is not a core focus of the research in this dissertation. Yet, throughout the research, concerns are raised about consumer surveillance by commercial platforms.

Consumer surveillance practices are embedded in platform ecosystems as they are mainly conducted via the infrastructures of big tech companies like Alphabet-Google, Apple, Facebook, Amazon, and Microsoft. Platforms (the aforementioned big five as well as many other companies) are programmable digital architectures *"designed to organise interactions between users – not just end users but also corporate entities and public bodies"* (Van Dijck et al., 2018, p. 4). Platforms are simultaneously technological, economic, and sociocultural configurations (Gillespie, 2010). Van Dijck et al. (2018) propose the concept of a platform society wherein societal, social, and economic traffic primarily moves via online platforms. In the platform society, private and public interest as well as commercial and public interests are almost always intertwined, while they are difficult to separate. The business models of most platforms rely on automatically collecting and processing user data, in order to target and profile individual users as well as user groups (Van Dijck et al., 2018). They thrive on consumer surveillance.

Consumer surveillance can be examined from multiple perspectives (Pridmore, 2012), some of which are detailed next. A *political economic* perspective frames consumer surveillance practices as part of informational capitalism. In this system, consumers are exploited by systems controlled by wealthy actors and socioeconomic interests steer consumer surveillance practices (Pridmore, 2012). In addition, a *modular* view on consumer surveillance focuses on the flexibility and (re)configuration of associations between data points. Databases allow for systematic modulations of consumer populations and how *"control and power operate in and through technological surveillance networks of contemporary information economies"* (Pridmore, 2012, p. 325). Political economy perspectives and modular views on consumer surveillance are visible in Zuboff's (2019) description of *surveillance capitalism* as a global political-economic system. Surveillance capitalism entails a society dominated by Internet companies (platforms) for whom consumer (behavioural) data form surveillance revenue which offers profits as well as informs markets in future behaviour (Zuboff, 2019). According to Zuboff (2019), this system threatens human autonomy and freedom by subjecting people to maximised extraction of personal data and using this to influence their actual behaviour.

A different critical focus on consumer surveillance is offered by a *contingent* approach with the relational aspects of corporate informational power as the main focus (Pridmore, 2012). In this view, marketing can be seen as a dynamic and iterative form of surveillance. Furthermore, *normative* accounts of consumer surveillance reflect on the implications of surveillance practices. These implications indicate that privacy is at stake, that there is a lack of corporate transparency, and that problematic forms of automated decision-making cause potential for cumulative disadvantage (Pridmore, 2012). Inaccurate, arbitrary, and biased algorithmic decisions based on digital profiles can limit chances and choices of not only individuals but of whole population groups (Christl, 2017).

However, *"there is a wide gap between what is theoretically possible and desirable with the tools and techniques that are employed in marketing contexts"* (Pridmore, 2012, p. 328). Throughout the research in this dissertation, questions are raised that are informed by political economic, normative, and contingent views of consumer surveillance. Chapter 7 provides insights into how privacy concerns around household IPAs focus on platforms. In the conclusion, I also reflect on the general role of platform ecosystems and commercial monitoring in everyday experiences of privacy and surveillance.

Lateral surveillance as a form of social surveillance

Surveillance practices are not limited to institutions or companies because individuals can engage in *self-surveillance* (e.g., via fitness tracking devices) (Esmonde, 2020). People can also monitor one another in horizontal and mutual processes which are described as *lateral surveillance* (Andrejevic, 2002, 2007), *co-veillance* (Mann, 2016), *role relationship surveillance* (Marx, 2015b), or *interpersonal surveillance* (Trottier, 2012). Andrejevic (2002, p. 488) defines lateral surveillance as *"peer-to-peer monitoring, understood as the use of surveillance tools by individuals...to keep track of one another, [lateral surveillance] covers (but is not limited to) three main categories: romantic interests, family, and friends or acquaintances".* In this dissertation, the term lateral surveillance is used. Chapters 3 and 8 provide novel insights into lateral surveillance practices in collapsed physical/digital contexts.

Existing research about lateral surveillance mainly focuses on interconnected technologies, such as instant messaging, cell phones, search engines, home surveillance products and services, and social media (Andrejevic, 2002; Lee et al., 2017; Trottier, 2012). The concept *social surveillance* is coined by Marwick (2012) to describe how reciprocal lateral surveillance practices on social media not only involve watching others but also a high awareness of being watched. More specifically, lateral surveillance via social media can result in self-censorship and chilling effects (Manokha, 2018). Because of the scrutiny and the internalised gaze of social media audiences, people refrain from posting potentially offensive or sensitive information that reveals their religious beliefs, political opinions, health, or sexual orientation. Also, extended chilling effects can occur when people constrain their offline behaviour in fear of pictures or videos being uploaded to social media (Manokha, 2018). However, interpersonal surveillance practices are not merely negative. Albrechtslund (2008) emphasises that mutual and horizontal surveillance practices, described as *participatory surveillance*, can also empower users when it supports their identity construction, enables them to meet friends and colleagues in different ways, and to socialise with strangers online.

While not studied often, non-digital forms of monitoring also play a role in lateral surveillance. An example is provided in research about interpersonal surveillance experienced by mothers (Henderson et al., 2010; Simmons, 2020). These authors provide examples of how mothers encounter monitoring by other mothers through interpersonal communication, (silent) observations, and social media. To add to this broader approach to lateral surveillance, Chapter 3 presents a practice theory-oriented perspective on lateral surveillance by showing how it is exercised in digital and non-digital contexts simultaneously (e.g., neighbours can check if their fellow WNCP participants have been online on WhatsApp and can also peek through their windows to see if they are home). Moreover, Chapter 8 studies family surveillance and emphasises some reciprocal or lateral elements in monitoring practices that take place in digital and non-digital forms.

Research setting

This PhD project is part of the *Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems* project, an international collaborative effort of the Erasmus University, the University of Maryland (US), and the University of Wisconsin-Milwaukee (US) which is funded by the NWO (NL) and NSF (US). Whereas the project also includes cross-national elements, this dissertation discusses privacy and surveillance experiences in Dutch contexts. The privacy of Dutch citizens is regulated via the European General Data Protection Regulation (supplemented by the Dutch Implementation Act (AVG) and supervised by the Dutch Data Protection Authority). In order to present a brief overview of Dutch privacy and surveillance practices and perceptions, I turn to survey reports and a content analysis.

Dutch people have a comparatively strong understanding of European legal mechanisms. 87% of Dutch respondents heard about the GDPR, and 60% claim they know what it is – ranking second highest of all 28 European countries included in a 2019 Eurobarometer survey. More specifically, 82% of the respondents are aware of the GDPR, the existence of a national public data protection authority, and their privacy-related rights (Kantar, 2019). However, knowledge about regulations does not guarantee trust in data protection regulation as only 42% of a representative sample of the Dutch population believes that the GDPR provides better data protection (DDMA, 2021). Fewer than a third of the respondents feels in control over their personal data and almost all respondents (89%) want more control over the data they share with companies. However, the fact that only 49% of them always looks at the cookie banner indicates that the means currently available to exercise control are not sufficient (DDMA, 2021). In terms of taking steps to protect online privacy, Dutch users most often delete cookies, decline cookies, or delete their browsing history. They least often opt-out on websites or use tools to prevent tracking (Boerman et al., 2018).

When it comes to perceptions of surveillance, a content analysis of online reactions and newspaper articles about the NSA revelations reveals a variety of Dutch attitudes (Mols & Janssen, 2017). A Dutch indifferent stance toward privacy and surveillance (as often indicated by newspapers) is only visible in a fraction of the public debate. The most recurring frames about NSA surveillance show a demand for privacy controls and express fears of losing privacy altogether due to the increase of surveillance. The research findings presented in this dissertation show that daily practices entail more nuanced experiences of privacy and surveillance than those visible in survey responses and public debates.

Dissertation outline

In this introduction, I present community, communicative, and intimate contexts as places where people experience privacy and surveillance in relation to safety, boundaries, and control. The next chapter further unpacks the overarching research question: How do people experience privacy and surveillance in their everyday practices? The research in this dissertation is guided by a combination of constructivist grounded theory and practice theory as a methodological basis for in-depth interviews and focus groups. Chapter 2 describes the methodological choices, approaches, and strategies for each study, presents research management considerations, and offers a reflection on my role as a researcher.

As explained in this introduction, the empirical chapters of this dissertation are divided into three conceptual parts. Part 1 describes safeguarding practices in the context of community based WNCP groups with a focus on lateral surveillance (Chapter 3) and participatory policing (Chapter 4). Part 2 presents privacy and surveillance experiences in communicative contexts; Chapter 5 explores boundary sculpting practices around absence/presence and relational contexts and Chapter 6 defines information boundary management strategies within workplace communication. Part 3 reflects on household IPA privacy concerns (Chapter 7) and family surveillance (Chapter 8) with a specific focus on practices of control in intimate contexts. Finally, the conclusion in Chapter 9 ties together the findings of the empirical chapters by explaining how everyday experiences of privacy and surveillance revolve around tangible negotiations. In the conclusion, I also reflect on the contributions of this dissertation on academic, empirical, and practical levels, discuss the limitations, provide insights into how the findings potentially extend to other contexts, and pose directions for future research.

Chapter 2

Methods and materials
Researching privacy and surveillance experiences

Introduction

In this dissertation, studying privacy and surveillance experiences entails collecting personal accounts of everyday practices in community, communicative, and intimate contexts. In order to provide nuanced insights into mundane practices, this research is informed by two approaches. A constructivist grounded theory method (Charmaz, 2014; Corbin & Strauss, 1990) and a practice theory lens are applied to analyse sociomaterial experiences (Gherardi, 2017; Schatzki, 2005). This chapter starts with a concise overview of the origins of constructivist grounded theory and of practice theory as a methodological approach. Afterwards, I present the sampling procedures followed by a description of the interview and focus group design, a justification of the analysis, and the data management and research integrity considerations.

Following a constructivist grounded theory approach

While used often, applications of grounded theory range from purist data-driven theory development to inductive analyses roughly inspired by grounded theory. I adopted a pragmatic and thorough research protocol based on constructivist grounded theory in this dissertation. To establish what this means, I first provide a brief overview of its origins starting with Glaser and Strauss' (1967) introduction of grounded theory as a response to positivist quantitative research approaches. In their work, they provide practical systematic guidelines to challenge the image of impressionistic and unsystematic qualitative research in social science. Grounded theory views data as the starting point for the development of theory because *"generating a theory involves a process of research"* (Glaser & Strauss, 1967, p. 6). Furthermore, this approach is based on theoretical sampling; simultaneous data collection, analysis and theory development (Glaser & Strauss, 1967). While the groundwork is established in a joint effort, Glaser and Strauss each provide their own version of grounded theory.

The main differences between their conceptualisations focus on the role of the researcher, the (timing of) theory, research questions, data coding, and data analysis (Howard-Payne, 2016). More specifically, Glaser's post-positivist grounded theory assumes an objective researcher whereas Strauss' constructivist grounded theory envisions a personally engaged researcher. And while Glaser proposes that a literature review needs to be conducted after the analysis and that literature verification can only take place via subsequent quantitative research, Strauss opts for a partial review of literature beforehand, together with literature verification via constant comparisons. Furthermore, Glaser refrains from using pre-set research questions, while Strauss bases research questions on existing literature. Finally, according to Glaser, grounded theory coding and analysis entails initial coding and comparisons, while Strauss recommends open coding with categorisation via axial coding (Howard-Payne, 2016).

I followed Strauss' constructivist grounded theory approach because it allows the use of theory for the development of research directions and questions. This, in combination with a three-stage coding procedure, is useful for providing an in-depth understanding of social experiences. The works of Corbin and Strauss (1990) and Charmaz (2014) form the main sources of inspiration for my research based on qualitative coding. Charmaz describes coding processes as:

> *"We study our early data and begin to separate, sort, and synthesise these data through qualitative coding. Coding means that we attach labels to segments of data that depict what each segment is about. Coding distils data, sorts them, and gives us a handle for making comparisons with other segments of data. Grounded theorists emphasise what is happening in the scene when they code data." (Charmaz, 2014, p. 3)*

Coding processes are an iterative process because the researcher constantly needs to compare new data with other (preceding) data. This process of constant comparison needs to be continued until the codes are saturated and new data does not lead to new codes (Boeije, 2002). In practice, rather than starting my research with writing theoretical frameworks which provide definitive concepts to prescribe the focus of the analysis, I engaged in the scoping of literature to find sensitising concepts as starting points for inductive research. I used these sensitising concepts as inspiration for my interview guides and added additional concepts during the research process on the basis of the research data (Bowen, 2006, building on Blumler, 1954). In Chapter 6 for instance, Petronio's (2012) communication privacy management (CPM) theory sensitised me to the fact that people actively manage the disclosure of private information. However, it was not until the final stage of the analysis that I connected CPM concepts like privacy rules to the respondents' experiences and completed the theoretical framework.

The section about the analysis procedures (later in this methods chapter) details how constructivist grounded theory guides the three-phase coding procedure used for my research. Below I briefly indicate how constructivist grounded theory coding proved to be particularly useful for studying privacy and surveillance experiences. The three-phase coding procedure is based on open, axial, and selective codes and provided me with the means to approach (descriptions of) many different everyday practices in a structured manner. I broke them down in all their complexities via open coding in the first phase. Second, I built them back up by establishing overarching categories (axial coding) in which I grouped similar codes. To illustrate, in the analysis for Chapter 8, all the experiences of parents and children were broken down to 397 open codes (see Appendix 15).

In the axial coding phase I found overlap in different forms of active family surveillance practices; parents monitoring their child's location, parents consulting student tracking systems, and parents checking their child on social media. These practices are different in nature but fit together under the axial code *monitoring embedded in everyday life*. Afterwards, the axial codes helped to make sense of the respondents' everyday experiences in a few main themes (phase 3) whereby *monitoring embedded in everyday life* became part of the selective code *providing safety & guidance*. In sum, constructivist grounded theory provides a reflexive research method with a pragmatic use of theory that is particularly helpful to analyse versatile everyday experiences.

Looking through a practice theory lens

When it comes to everyday experiences of privacy and surveillance, the introductory chapter of this dissertation emphasises that what people do is more telling than what they say. In other words, it is more fruitful to study practices than beliefs. In order to do this effectively, the second methodological approach of this research is provided by practice theory which aims to understand social life through practices (Schatzki, 2002). Before introducing practice theory, I present sociomateriality as an important foundation that establishes the importance of material elements in practices. Sociomateriality indicates that the social and the technical are inseparable within practices and because practices exist of matter and culture (Gherardi, 2017). As Orlikowski states; *"the social and the material are constitutively entangled in everyday life" [emphasis in original]...humans are constituted through relations of materiality; bodies, clothes, food, devices, tools, which, in turn, are produced through human practices"* (2007, p. 1437).

Sociomateriality entails the interdependence of social and material dimensions of everyday practices. I take these considerations into account by highlighting how sociomaterial privacy and surveillance experiences entail an interplay between social and material elements. Chapter 5 for instance describes how people actively sculpt boundaries between relational contexts. While this is a socially oriented practice, the analysis highlights how boundaries are shaped through material elements like mobile phones and specific digital settings. In the empirical work in this dissertation, attention to sociomaterial dimensions provides new insights into how digital interfaces and features are paramount to privacy and surveillance practices.

Sociomateriality lies at the heart of practice theory, a theoretical approach proposing that practices form the building blocks of social order (Schatzki, 2002). Practices can be defined as *"embodied, materially mediated arrays of human activity centrally organised around shared practical understanding"* (Schatzki, 2005, p. 11). Notably, *materially mediated* refers to how practices are interwoven with material and embodied elements, relating sociomateriality to the fact that objects form constitutive components of practices (Reckwitz, 2002). Reckwitz presents a practice as a *"routinised type of behaviour which consists of several elements, interconnected to one another: forms of bodily activities, forms of mental activities, 'things' and their use, a background knowledge in the form of understanding, know-how, states of emotion and motivational knowledge"* (Reckwitz, 2002, p. 248). These definitions are reconceptualised by Shove et al. (2012) who argue that practices come into being when three interconnected dimensions interact, namely c*ompetencies, meanings,* and *materials.* The material dimension refers to objects or *things* paramount to practices, such as tools, objects, hardware, infrastructures and bodies. According to Schatzki (2002), most actions cannot take place without objects. In this dissertation, the material dimension of privacy and surveillance practices include tangible, digital, human, and non-human elements, such as smartphones, smart speakers and appliances, laptops, digital interfaces, messaging apps, and bodies.

To successfully engage in practices, an *"understanding and practical knowledgeability"* is required (Shove et al., 2012, p. 23). This competence dimension is presented includes know-how, background information, and practical skills along with rules, principles, and explicit instructions (Schatzki, 2002; Shove et al., 2012). For privacy and surveillance practices, this can entail practical knowledge about particular functionalities of messaging apps, knowledge about which data are collected by media platforms, an understanding of the workings of GPS tracking applications, or know-how about how to connect, and set-up smart home technologies. Moreover, an awareness of social norms and reflexivity towards the consequences of practices can also be part of privacy and surveillance practices. To illustrate, when someone *keeps an eye on their neighbour* this might be a socially acceptable practice when it is done by occasionally checking the street, but is probably not considered acceptable when someone uses binoculars to look into a neighbour's living room. This example shows how practices entail tacit knowledge of social norms.

The material and the competence dimensions would not be carried out without a particular purpose. Meaning can be understood as the social and symbolic significance of practices (Shove et al., 2012). The privacy and surveillance experiences studied in this dissertation include meaning dimensions that overlap as well as divert. For example, parental monitoring practices (Chapter 8) have a social and symbolic significance in their goal of safeguarding children, while WNCP practices (Chapters 3 and 4) are meaningful in their purpose to safeguard the neighbourhood. When it comes to boundary management practices (Chapters 5 and 6), meanings range from maintaining personal connections to protecting personal information and intimate contexts. And household IPA privacy practices (Chapter 7) revolve around convenience and control.

Practices are often not limited to one location; they can be seen as co-located practice bundles emerging in different contexts (Shove et al., 2012). (Dimensions of) practices shape each other and change over time. Christensen and Røpke (2010) note how change to practices is brought by internal factors like experimentation and improvisation of practitioners and by external factors such as adjacent practices, institutional arrangements, economic situations, and technological innovations. In this dissertation, I build on the work of Reckwitz (2002), Schatzki (2005), and Shove et al. (2012) and use practice theory as a methodological approach to study privacy and surveillance practices as sociomaterial activities driven and motivated by particular knowledge, competence, and meanings The privacy and surveillance practices in this research are studied at one point in time; however, I reflect on how they have changed or might change.

Practice theory as a methodological approach

Whereas the abovementioned authors contribute to theories of practice, revising or reconceptualising practice theory is not the goal of this dissertation. Instead, practice theory provides a methodological approach because I perceive everyday technology use as an assemblage of sociomaterial practices. Studying practices means shifting social analysis from individuals to practices, whereby the focus lies on doings taking place in specific situational settings. This approach guides the researcher *"back to the social roots of meaningful experience"* (Woermann, 2017, p. 156). Instead of focusing on opinions or attitudes, the focus lies on what people do and how their practices are inherently social as well as inherently material. With the goal of focusing on the social and material dimensions of meaningful activities, practice theory is embedded in the empirical research of this dissertation. Specifically, throughout the process of constructing interview guides and topic lists, talking to respondents in focus groups and interviews, analysing the transcripts, and reporting the most prevalent findings, I was most attentive to what people do rather than what they think, believe, or know.

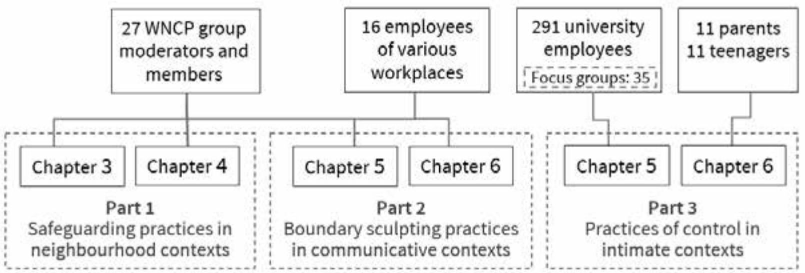
When respondents describe how they use materials such as smartphone-based messaging apps or apps to monitor their children, they automatically touch upon the materials included as well as the social considerations behind their practices. It is not that individual beliefs, perceptions, and opinions are not interesting; rather it tells much more when it is clear how these are embedded in sociomaterial activities, social contexts, and patterns of reproduced practices. For instance, in a focus group discussion in wealthy neighbourhood with many recent house break-ins, Lucia (WNCP group member) mentioned that messages in the WNCP group can make her anxious. She states, *"Well, if it [a person acting suspicious] is as close by as last time… I was really terrified. I always sleep with the windows open, we sleep at ground floor level with the windows open, but then I close the windows".* This quote indicates how for Lucia, the WNCP group that she generally appreciates can also make her anxious which leads to closing her windows at night to create physical protection from potential dangers. By focusing on practices, the sociomateriality of Lucia's anxiety becomes visible in how she constructs physical protection against a risk that materialises via social WhatsApp interactions. This example shows how the focus on sociomaterial practices enables an analysis of experiences as meaningful assemblages of material and social dimensions.

A practice theory approach forms the basis of all interview and focus group guides and plays a role in the six empirical studies in this dissertation. The application differs from watchfulness practices structured along practice theory elements (Chapter 3), insights into participatory policing practices (Chapter 4), to practice theory elements as sensitising concepts in the analysis of privacy management and boundary work (Chapters 5 and 6), to a focus on the sociomateriality of (anticipated) smart speaker use (Chapter 7) and family surveillance practices (Chapter 8).

Neighbours, employees, and families: Data collection

For this dissertation, I recruited 100 respondents for interviews and focus groups and 291 survey respondents. All these respondents were selected with a particular goal, purposive sampling was used to recruit information-rich units of analysis aiming for maximised diversity (Patton, 1990). This way, I was able to reach a great depth of information via a relatively small number of participants per study (Teddlie & Yu, 2007). Moreover, my purposive sampling procedures can also be described as selective sampling (Coyne, 1997) because the criteria for the selection of new respondents were developed along the way. In other words, the interviews took place in waves and after each wave, I reflected on the topics discussed in order to determine what additional types of respondents were needed to maximise variety in the samples. The respondents are presented in Figure 2 and below I outline the specific sampling and recruitment procedures for each study.

Figure 2. Overview of respondents and chapters


27 WNCP group moderators and members
16 employees of various workplaces
291 university employees
Focus groups: 35
11 parents
11 teenagers
Chapter 3
Chapter 4
Chapter 5
Chapter 6
Chapter 5
Chapter 6
Part 1
Safeguarding practices in neighbourhood contexts
Part 2
Boundary sculpting practices in communicative contexts
Part 3
Practices of control in intimate contexts

For the first study about WNCP groups, I conducted 14 interviews with WNCP group moderators and two focus groups with 11 WNCP members in the first six months of 2017. The respondents were recruited via my (extended) personal and professional network, social media (public and private messages on Twitter and LinkedIn), an online directory of WNCP groups (https://wapb.nl), and snowball sampling. The diversity of WNCP networks, the range of potential motivations and experiences of members, and the novelty of these practices demand an in-depth qualitative understanding of WNCP practices. I analysed the interview data directly after the interviews, which allowed for theoretical sampling. In theoretical sampling, data collection and analysis take place simultaneously and specific data are sought in order to develop emerging theory (Charmaz, 2014; Glaser & Strauss, 1967).

More specifically, the analysis of the first interviews with moderators of large WNCP groups resulted in coding categories about large-scale WNCP practices in suburban neighbourhoods. With the goal of building theory about participatory policing and lateral surveillance in a broad variety of WNCP contexts, moderators of small WNCP groups and WNCP groups in a variety of neighbourhood contexts were recruited (villages, towns, cities, and suburbs). Subsequently, after the analysis of these interviews, some initial categories were developed around (a lack of) police involvement, which led to a third wave of interviews within WNCP groups that included community police officers. And finally, after the interviews, I analysed the experiences in WNCP groups based on moderator views but felt that the perspectives of members were needed to provide insights into how citizens experience these groups. Therefore, two focus groups were organised. Appendix 1 lists the (pseudonymised) interview and focus group participants, gives an indication of the type of neighbourhood they live in, and provides information about the involvement of police in their groups. These interviews and focus groups form the basis for Chapters 3 and Chapter 4 (the latter also includes 13 additional interviews with WNCP moderators and members conducted by a master student). Figure 2 indicates that parts of the interviews and focus groups are also used in Chapter 5.

The second round of data collection entailed interviews with employees of a variety of workplaces and took place in Spring 2017. These interviews are used in Chapters 5 and 6 about boundary management practices. Given the potential diversity of digital workplace communication, I aimed for maximised diversity by recruiting respondents in different jobs and professional roles. The 16 interview respondents are (self-)employed by a start-up, software firm, graphic design agency, multinational, hotel, government, consultancy firm, municipality, restaurant, and a zoo. The sample includes five office employees, four self-employed professionals, three service-industry employees, and four managers in different types of companies (see Appendix 2). Moreover, the sample includes people with desk-jobs (the office employees, self-employed professionals, and two of the managers) and service industry employees (the other two managers and the restaurant employees). The three restaurant employees were interviewed together in a small-scale focus group setting. Similar to the WNCP study sample, respondents were recruited via public and private messages on LinkedIn and Twitter, via my (extended) personal network, and the networks of the respondents (snowball sampling). All respondents for the first two rounds of interviews and focus groups received a chocolate bar as a token of appreciation for their participation.

Whereas most samples in my dissertation are based on purposeful sampling aimed at maximised diversity, this was not the case for the mixed-methods study about smart speakers in Chapter 7. This chapter exists of an exploratory survey followed by six semi-structured focus groups which together provide an in-depth and multidimensional understanding of household IPA privacy concerns. The qualitative focus group data is used to explain the initial results of the quantitative survey data, adopting an explanatory sequential design (Creswell & Plano Clark, 2017). This particular study was part of a cross-national comparison between US and NL privacy attitudes around Intelligent Personal Assistants (in the contexts of the Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems project). Therefore, the sample and the survey were constructed in close collaboration with the US partners. In April 2018, I distributed a survey via email to 3000 employees of a university in the Netherlands, including university staff as well as research personnel (see Appendix 7 for the survey). A total of 325 respondents participated in the survey out of which 291 completed the questionnaire resulting in a response rate of 10%. As an incentive to complete the survey, participants could enter their email address to participate in a raffle for one of five €50,- Bol.com gift vouchers. The survey was also used as a recruitment tool for the six focus groups and allowed for the recruitment of 35 university employees in a variety of professional roles (see Appendix 3). As an incentive, all focus group participants received a €10,- Bol.com gift voucher.

The final study focused on 9 families and includes interviews with 11 parents and 11 early adolescents between 11-15. In order to reach maximised diversity in the sample, families with different set-ups were included (such as nuclear families, one-parent families, and a foster care family). The families were recruited via my (extended) personal network, and I conducted the interviews in three waves in Spring 2021. After each wave, I consulted my notes and recruited three new families on the basis of perspectives that were still lacking (for example, after interviewing the mother and daughter of a one-parent family with one child, I was curious whether similar considerations would be visible in other one-parent families with more children and therefore recruited a one-parent family with three sons). The family interview respondents received a gift voucher from a (web)shop of their choice of €15 for each completed interview.

Interviews and focus groups about practices

All the interviews and focus groups in this dissertation observed a similar procedure. They were semi-structured and designed in anticipation of inductive, bottom-up analyses. The semi-structured interviews were each based on a fixed set of questions providing me with the flexibility to pose follow-up questions and vary in the order of topics (Brennen, 2013). Key to constructing the interview and focus group guides was a focus on practices (see Appendices 5 to 8), I asked the respondents how they use technologies and applications in their everyday lives. As mentioned before, taking practices as a starting point allowed for an exploration of sociomaterial technology uses and interactions.

I used intensive interviewing, a form of interviewing guided by open-ended, non-judgmental questions which *"permits an in-depth exploration of a particular topic or experience and, thus, is a useful method for interpretive inquiry"* (Charmaz, 2014, p. 25). Intensive interviewing is particularly useful in constructivist grounded theory research because both have an open-ended yet directed character, are shaped yet emergent in nature, and is paced yet unrestricted (Charmaz, 2014). The open-ended and exploratory nature of the interviews enabled me to use the same interview data for multiple analyses (e.g., three different analyses of the WNCP interview transcripts resulted in Chapters 3, 4, and 5). Below I detail the specifics of the four waves of interviews and focus groups.

The first wave of WNCP interviews and focus groups covered a diverse range of topics; the start and development of the WNCP groups, guidelines, examples of successful events and failures, monitoring practices, administrative efforts, general use of messaging apps, and practices to manage availability (see Appendix 5). The two focus groups and most interviews were conducted face-to-face (with the exception of two interviews done via telephone and Skype) and on average, the interviews lasted 70 minutes and the focus groups 95 minutes. In order to elicit reactions about possible consequences of WNCP groups in the focus groups, I prompted the respondents with news articles about beneficial and disadvantageous uses of WNCP.

Workplace communication practices, the use of enterprise social media, personal social media practices, and messaging app interactions were the main themes in the second wave of interviews (see Appendix 6). Eleven of these interviews were conducted face-to-face, two via telephone. The interviews with employees were one-on-one and took 60 minutes on average, however, one interview with three participants lasted 90 minutes.

The third wave of empirical research revolved around six focus groups with 35 university employees. Focus groups proved to be a particularly helpful research method because household IPAs were not yet on the market at the time of the empirical research. Focus groups enable an exploration of perceptions (Stewart et al., 2007), in this case, the respondents engaged in discussions about how they use and perceive smartphone IPAs and household IPAs.

For the latter, I used two prompts to enable reflections on anticipated uses of such smart devices. First, I screened a commercial wherein multiple Google Homes are integrated in the life of a busy family. The second prompt makes that these sessions were focus groups rather than group interviews because they were *focused* on a collective activity (Kitzinger & Barbour, 1999). Namely, the respondents were invited to interact with a Google Home device that was installed in the focus group space and was connected to a lamp and a smart TV. I provided example prompts, such as *OK Google, what is the weather forecast?, OK Google, switch on the lamp,* and *OK Google, play Bruno Mars on Spotify.* In all focus group conversations, the actual practice of engaging with the smart speaker led to conversations about the device guided by questions about anticipated uses, benefits, drawbacks, and the connection to the Internet of Things (IoT) (see Appendix 7). Group interaction was used "*to produce* *data and insights that would be less accessible without the interaction found in a group"* (Morgan, 1997, p. 12).

Family life during the Covid-19 pandemic, social media practices and parental monitoring, family communication, and smart technology use formed the four themes of the final wave of interviews (see Appendix 8). While I designed one interview guide for the parents and one for the children, I interviewed the family members in different compositions. My main goal was to interview respondents in a situation wherein they felt comfortable, and I also had to adapt to the situation. Most interviews took place in an open kitchen/living room area with other family present who at times disrupted or intervened the interviews. Nine interviews were conducted face-to-face in family homes, and four interviews online via Zoom, Google Meet, and Teams. In some families, I conducted interviews with the parent(s) and the child(ren) separately, whereas in other families, they preferred to be interviewed together. The respondent overview in Appendix 4 includes a description of the interview settings.

Constructivist grounded theory analysis: Coding strategy

All interviews and focus groups were transcribed in a verbatim manner, and I analysed the transcripts via an iterative three-stage coding process. I used qualitative data analysis software (Atlas.ti) to do this in a systematic, transparent, and efficient manner. The first coding phase concerns open coding, an *"interpretive process by which data are broken down analytically"* and labels are constructed for specific data segments (Corbin & Strauss, 1990, p. 12). Key to this initial coding phase is to keep an open mind, to stay close to the data, construct short, simple, and precise codes, keep comparing the data, and move through the data quickly (Charmaz, 2014). I read all my interview transcripts carefully and I connected short labels (codes) to interview segments. I stayed close to the text by paraphrasing sentences into codes, and where possible by literally copying contents of a segment into a code – in other words, by making use of in-vivo coding (Charmaz, 2014).

This coding procedure was iterative because I constantly compared the applications of (similar) codes. This helped to break through subjectivity and bias (Corbin & Strauss, 1990); by zooming in and out on codes I was forced to reflect on potentially subjective and biased coding and to recode sections when needed. Moreover, temporarily separating the codes from the interview contexts helped me to check whether the codes were consistent and remained open. Examples of open codes are *keeping a distance* and *social control unwanted* in the WNCP interviews, *private message incident* and *separate work phone* in the workplace communication interviews, *household IPA always listening* and *household IPA like science fiction* in the IPA interviews, and *location tracking to locate parent* and *freedom child important* in the family interviews. Ultimately, many codes occurred often in different interviews and fewer new codes emerged, an indication that I reached theoretical saturation (Given, 2008).

The second phase of coding is axial coding (Corbin & Strauss, 1990): open codes are clustered together in overarching conceptual codes. For my research, I engaged in separate axial coding procedures for each of the six empirical chapters. All the open codes of the related interview transcripts were compiled and where needed I made selections. For instance, the analysis in Chapter 5 about boundary work is based on WNCP interviews and workplace communication interviews. For this analysis, I did not use the open codes about particular WNCP practices as I made a selection of 312 relevant open codes focusing on communication (see Appendix 12). For each chapter, I created clusters of open codes based on similarities. Some of these axial codes are conceptualised on the basis of existing literature and others on interpretations of the open codes. An example of such a mutually exclusive conceptual axial code from Chapter 6 about digital workplace communication is the *protecting personal time* axial code. This code is based on the conceptualisation that open codes like *phone not in bedroom*, *enable do-not-disturb mode*, and *vacation less online* are related because they all concern strategies to limit the presence of smartphone use in private time.

The third and final stage of the constructivist grounded theory coding process is selective coding; *"the process by which all categories are unified around a 'core' category, and categories that need further explication are filled-in with descriptive detail"* (Corbin & Strauss, 1990, p. 14). I reinterpreted these instructions because I constructed not one but multiple selective codes per analysis based on research questions. The reason behind this was merely pragmatic, the academic journals I aim for as outlets for my research require a solid theoretical basis and often also explicit research questions. Therefore, the theoretical frameworks and research questions form the basis for the construction of selective codes. For example, in Chapter 7 about household IPAs, the research question (informed by theory) is: *what role do affordances play in household IPA privacy concerns in the context of surveillance, security, and platforms?* In order to provide this question in a systematic manner, the axial codes were clustered along surveillance, security, and platform concerns (see codebook in Appendix 14).

Research management and integrity

Throughout the empirical research for this dissertation, research integrity was guaranteed in the contact with respondents, the handling of their data, the analysis process, and writing up the results. First and foremost, all studies of this dissertation were approved by the ethical review board of the Erasmus School of History, Culture and Communication. These review processes included a review of the consent forms, benefits and risks, data management plan, and research design.

Before the start of the interviews and focus groups, all respondents signed informed consent forms describing the research procedures, the absence of physical, legal, and financial risks, a description of potential benefits (such as new insights into data collection and technology use), information about the incentives, data collection and processing, pseudonymisation, the opportunity to retract participation, where to direct questions or complaints, and the opportunity to be informed about the research findings. Moreover, the respondents were explicitly asked for consent for an audio recording. Consent was provided on paper or verbally during the interviews. Examples of the consent forms are included in Appendix 9.

All interviews and focus groups were audio recorded, transcribed, and prepared for analysis and I took measures to protect the personal information of the respondents and interview data. Where possible, I followed the principle of data minimisation and only stored the first names and one phone number or email address for the respondents. Superfluous information was deleted as soon as possible, for instance, when respondents shared their address for an interview at their house, I deleted this information directly after the interview. Almost all transcriptions were done by third parties, who signed confidentiality agreements. The interview recordings, transcripts, and analysis documents were safely stored in an online password protected document vault (a service offered by the Erasmus University) or SURF drive (a personal cloud service for Dutch education and research). All transcripts and other research data will be destroyed according to the timeframe indicated in the consent forms. Moreover, almost all interviews and focus groups were conducted in Dutch, apart from one interview and one focus group that were conducted in English. Relevant Dutch quotes were translated into English. Pseudonyms are used to protect the privacy of respondents and information that can be retraced to individual respondents was left out of the empirical chapters (such as the names of neighbourhoods, schools, or workplaces).

My research findings did not emerge by themselves but, rather, I made conscious decisions as a researcher. This process was influenced by my position as an interdisciplinary researcher with a background in media studies, communication, and sociology. The findings and conclusions that I present in this dissertation are interpretations informed by my views (Charmaz, 2014). Gherardi (2017, p. 48) states that researchers should be responsive of how the distinctions we make influence our experiences and *"conceal as well as reveal what we research in the practices that we study".* I interpret these considerations as the need to reflect on the decisions I made (in selecting particular theories, in coding particular interview snippets with short in-vivo codes, in clustering specific groups of codes, in presenting a selection of interview findings, and in connecting those to literature), and on how these influence my conclusions and the storyline of this dissertation.

Throughout the dissertation, I try to be mindful of how my decisions shape the outcomes, and to show reflectiveness of how the findings are partly determined by my decisions as well as their situatedness in empirical research contexts. Moreover, by making the research process transparent via the interview guides and codebooks in appendices 5-8 and 10-15, I hope to provide sufficient insight into how I constructed my argumentation and reached conclusions. Finally, following Charmaz' (2014) principles for constructing grounded theory, I aimed to ensure credibility by providing detailed descriptions of the situated practices to achieve familiarity with the research topics, to provide enough depth to merit my claims, to engage in systematic comparison between interview data and conceptual categories, to *"cover a wide range of empirical observations"* (Charmaz, 2014, p. 182), to make the links between data and argumentation logical, and to provide enough evidence for a reader to form an independent assessment.

Having established the theoretical basis in the introductory chapter, and the methodological foundation in this methods chapter, the next chapter forms the start of the empirical section of this dissertation. In the three following parts, I present the results of six studies that each focus on a particular aspect of everyday experiences of privacy and surveillance related to safeguarding practices, boundary sculpting practices, and practices of control.

PART 1

Safeguarding practices in neighbourhood contexts

Chapter 3

"A sense of security" Dimensions of WhatsApp neighbourhood crime prevention practices[2]

Introduction

> *"When there are cars in the neighbourhood we are not familiar with, or when we are not sure about people we have never seen before, we'll take a picture and send it: Do we know anything about this?"* (Pauline, WNCP moderator)

Pauline is the moderator of a WhatsApp neighbourhood crime prevention (WNCP) group in a city in the Netherlands. As indicated in the introductory chapter, WNCP groups are WhatsApp conversations among neighbours which are used to exchange warnings, concerns, and information about incidents, emergencies and (allegedly) suspicious situations in the community. Pauline's quote shows that she and her neighbours immediately materialise such suspicions into pictures of unfamiliar vehicles or persons which they share in the neighbourhood WhatsApp group. This provides a preview into how voluntary citizen participation in crime prevention practices has inherently ambivalent consequences. Needless to say, WNCP-related watchfulness practices impact the experiences of neighbours as well as passers-by.

For neighbours, participants, and non-participants, an active WNCP group can change the neighbourhood dynamic into a watchful, and at times distrustful, atmosphere. And even if there are street signs signalling the existence of a WNCP group, passers-by are often

[2] This chapter is a slightly altered version of: Mols, A. (2021). Citizen Participation in Community Surveillance: Mapping the Dynamics of WhatsApp Neighbourhood Crime Prevention Practices. In H. Rahman (Ed.), *Human-Computer Interaction and Technology Integration in Modern Society* (pp. 157–176).

unaware of the fact that they are actively being monitored by citizens. It is important to note that surveillance practices existed in neighbourhoods long before WNCP initiatives emerged. Alert neighbours who keep an eye out on the street and who contact neighbours or police in case of trouble are not a new phenomenon. However, the use of WhatsApp (or similar messaging applications) has changed neighbourhood interactions and practices. Communication technologies are known for creating new forms of interaction in neighbourhoods (Hampton, 2007). The emerging use of WhatsApp groups within existing surveillance practices is currently changing neighbourhood dynamics and personal experiences, which makes this a pressing issue. This chapter questions **how WhatsApp conversations amplify neighbourhood watchfulness practices and incite forms of lateral surveillance**.

WNCP practices are a form of informal surveillance, the *"casual, but vigilant, observation of activity occurring on the street and active safeguarding of property"* (Bellair, 2000, p. 140). Notably, these practices can also be seen as forms of lateral, or interpersonal surveillance (Andrejevic, 2002; Trottier, 2012) because people actively monitor their peers, or in this case, their neighbours. The goal of this chapter is to understand smartphone-driven informal surveillance activities through the lens of practice theory. As discussed in Chapter 2, practice theory aims to explain society, culture, and social life through practices. Practices are not static but change over time (Reckwitz, 2002; Schatzki, 2002; Shove et al., 2012). This makes practice theory particularly suitable to study societal developments such as the impact of the emergence of WNCP groups on neighbourhood dynamics.

This chapter maps the consequences of a citizen initiative aimed at improving safety and shows that surveillance practices in WNCP groups have emerged in different forms and shapes. By highlighting the diversity in WNCP practices and the fact that this phenomenon is still developing, we found that neighbours are improvising on a daily basis in their self-organised WNCP groups. Interviews and focus groups revealed how friction in the conjunction of dimensions in WhatsApp neighbourhood watchfulness practices affects the personal lives and experiences of people (often unknowingly) involved. In the results section, we offer an in-depth account of the sociomaterial elements assembled together in everyday neighbourhood watchfulness and surveillance practices. Pressing issues related to lateral surveillance, participatory policing, and the normalisation of distrustful and intolerant attitudes are highlighted. The use of practice theory shows a co-constructed amplification of watchfulness practices revolving around a technical layer (WhatsApp) that brought qualitative change to existing neighbourhood practices and experiences. Despite a more or less unified articulation of purpose – protecting neighbourhoods – differentiations became visible across enacted neighbourhood watchfulness practices. Rather than avoiding these complexities, these tendencies are explored in clusters of actions and materialities. This chapter not only addresses the pressing nature of the issues arising in emergent WNCP activities in a specific local context, it also offers an exploration of lateral surveillance practices which go beyond digital forms of monitoring.

Literature: Participatory policing and lateral surveillance

WNCP practices can be seen as a form of (lateral) surveillance taking place in a Dutch context. In the results section of this chapter, clusters of WNCP practices are presented. In the descriptions of these clusters, specific practices are connected to relevant literature. This literature section provides overarching research and literature as a theoretical and practical background for the results section. First, I discuss how WNCP groups relate to neighbourhood block watch groups. Second, privacy concerns and lateral surveillance are discussed, and third, WNCP groups are presented as practices.

Neighbourhood watchfulness practices in the Netherlands

In the previous three decades, the Dutch government's approach shifted from active governance to regulations wherein citizens are co-producers of safety (Van der Land et al., 2014). Safety has become a shared responsibility of police and citizens. Similar to neighbourhood watch initiatives in other countries, neighbourhood block watch groups are active in the Netherlands. A recent inventory found 661 block watch groups in the Netherlands (Lub, 2018). Block watch revolves around small groups of participating citizens devoting their time to neighbourhood safety. The employment of WhatsApp for neighbourhood watch purposes radically increased the number of actively monitoring citizens in the Netherlands. The fact that there are more than 9,000 registered WNCP groups in the Netherlands (see the overview on https://wapb.nl) shows that WNCP groups not only supplement but more often supplant physical neighbourhood watch groups. Building on the description of WNCP groups in the introductory chapter, it is important to note that police are often not involved in neighbourhood safeguarding and surveillance practices (Mehlbaum & Steden, 2018). In order to make sense of the inherently conflicting nature of WNCP practices with their beneficial as well as detrimental consequences for neighbourhood dynamics and personal experiences, this chapter zooms in on sociomaterial practices as citizen-initiated surveillance activities.

Privacy and lateral surveillance in WNCP

The introductory chapter already mentioned that people's day-to-day life can be seen as being under constant surveillance, and according to Lyon (2007, p. 1), "*humans are surrounded, immersed, in computing and networked technologies from dawn to dusk in every conceivable location".* WNCP practices entail multiple forms of surveillance with each their own privacy-issues. First, the group conversations take place on WhatsApp, a commercial platform owned by Facebook. Whereas conversations might be protected by end-to-end encryption, unencrypted meta data still enable commercial surveillance of locations, connections, patterns, and personal information (Rastogi & Hendler, 2017).

Second, the potential involvement of police actors in WNCP groups can lead to surveillance by law enforcement, often without knowledge or consent of participants (see also Chapter 4). Finally, as indicated earlier, WNCP practices can be seen as a form of lateral, or peer-to-peer, surveillance (Andrejevic, 2002, 2007). WNCP practices entail a digital counterpart of lateral surveillance when participants view the information neighbours openly share on WhatsApp (phone number, profile picture, status update), or when they use WhatsApp to check if their neighbours are or have been online, and if they have read their messages. Moreover, moderators also often screen new participants on Facebook to check if they are trustworthy. However, most interestingly, WNCP practices offer a different layer to lateral surveillance practices when neighbours actively watch one-another in person. The combination of digital and non-digital interpersonal surveillance practices is further explored in the results section.

WNCP groups through a practice theory lens

WNCP surveillance activities can be seen as practices; routinised types of behaviour which entail configurations of interconnected dimensions (Reckwitz, 2002). When studying practices, the conjunction of the three interacting competence, meaning, and material dimensions should be taken into consideration (Shove et al., 2012, see Chapter 2). These form the lens through which WNCP group practices are analysed in this chapter. The *material* dimension refers to objects as constitutive components of practices (Reckwitz, 2002). Tools, objects, hardware, infrastructures and bodies are paramount to practices, as most actions cannot take place without objects (Schatzki, 2002).

Within neighbourhood watchfulness practices, the material dimension consists of physical streets and houses. Moreover, bodies are also material dimensions, in the form of citizens watching their street and passers-by who become (unknowingly) subject of watchfulness practices. Other material elements are the tools used by citizens to enhance their practice (binoculars), to collect proof of suspicious activities (cameras) and to contact police, neighbours, or others (phones). To successfully engage in neighbourhood watchfulness practices, specific knowledge is required. *Competence* refers to *"understanding and practical knowledgeability"* in the broadest sense, including know-how, background information, practical skills (Shove et al., 2012, p. 23) as well as rules, principles, and explicit instructions (Schatzki, 2002). The particular knowledge needed for watchfulness practices includes the capability to assess suspicious persons and activities, the knowledge of what is normal and what is deviant behaviour, and the skills to protect the street. Yet, the material and the competence dimensions would not be put to practice without a particular purpose. This is conceptualised in the *meaning* dimension which entails *"the social and symbolic significance of participation at any moment"* (Shove et al., 2012, p. 23). For neighbourhood watchfulness practices, this motivational knowledge is based on the desire for a sense of security and the purpose of safeguarding the neighbourhood. Also, it signifies the protection of private space and alertness.

Neighbourhood watchfulness practices are the result of particular configurations of material, competence and meaning dimensions. Neighbours are the practitioners producing, carrying out, and reproducing these activities, their shared practices form collective accomplishments (Barnes, 2001, p. 31). Neighbourhood watchfulness entails a bundle of practices including watching the neighbourhood, informing the police, taking action, and interacting with neighbours. These practices are not limited to one location, they can be seen as co-located practice bundles emerging in different neighbourhoods (Shove et al., 2012). In order to provide an in-depth account of watchfulness practices, a qualitative research design is used.

Research method: WNCP interviews and focus groups

The diversity of WNCP groups requires an in-depth qualitative understanding of the range of practices. Therefore, I follow a constructivist grounded theory approach (Charmaz, 2014). Semi-structured in-depth interviews and focus groups with 27 WNCP group moderators and members have been conducted, transcribed, coded, and analysed. Because WNCP groups exist in all types of neighbourhoods, sampling was aimed at maximised diversity on the basis of Statistic Netherlands' degree of urbanisation[3]. The urbanity level is included in the respondent overview in Appendix 1. The interview guide and codebook are included in Appendices 5 and 10 respectively and the methodological details can be found in Chapter 2.

Results: Neighbours' experiences of WNCP practices

As mentioned earlier, watchfulness practices existed in neighbourhoods long before WNCP initiatives first emerged. However, WNCP groups amplified existing surveillance practices because WhatsApp use changed the configuration of the three dimensions (material, competence and

[3] The full CBS Degree of Urbanisation scale, based on the surrounding address density: 1) Extremely urbanised: 2,500 or more addresses//km2; 2) Strongly urbanised: 1,500 to 2,000/km2; 3) Moderately urbanised: 1,000 to 1,500/km2; 4) Hardly urbanised: 500 to 1,000/km2; 5) Not urbanised: fewer than 500 /km2. (https://www.cbs.nl/en-gb/our-services/methods/definitions?tab=d#id=degree-of-urbanisation).

meaning). Monitoring practices have occurred before in assemblages of houses, streets, bodies, binoculars, and the physical watching practices of neighbours. When citizens wanted to communicate about activities on the street, they had to establish (one-to-one) phone connections or engage in physical conversations. In WNCP practices, these assemblages are amplified by Internet connections, (smartphone) cameras, and WhatsApp groups which enable neighbours to reach all members of their group instantaneously in order to inform or activate them. The seemingly invisible Internet infrastructures manifest itself in connectivity icons and the WhatsApp interface on smartphones and other devices. With cameras embedded in smartphones, pictures can immediately be shared with neighbours, police, and others.

Thus, the expanded material dimension directly enhances WNCP practices because participants have gained the facilities to activate and inform neighbours and police more effectively than before the use of WhatsApp. However, the competence dimension also changed because participating in WNCP practices requires skills that were not needed before. Namely, citizens need to know how to use their smartphone, to install WhatsApp, and to communicate with their neighbours. Furthermore, the meaning component now includes connectivity, which is indispensable for the continuous communication with neighbours.

Distinctions in competence and meaning dimensions

When WhatsApp groups were integrated in neighbourhood watchfulness and surveillance practices, a reconfiguration of the three dimensions took place. During the interviews it became clear that, while the material dimension of WNCP practices has similar aspects across groups, WNCP groups were different in their competencies and in the meaning they attributed to their practices.

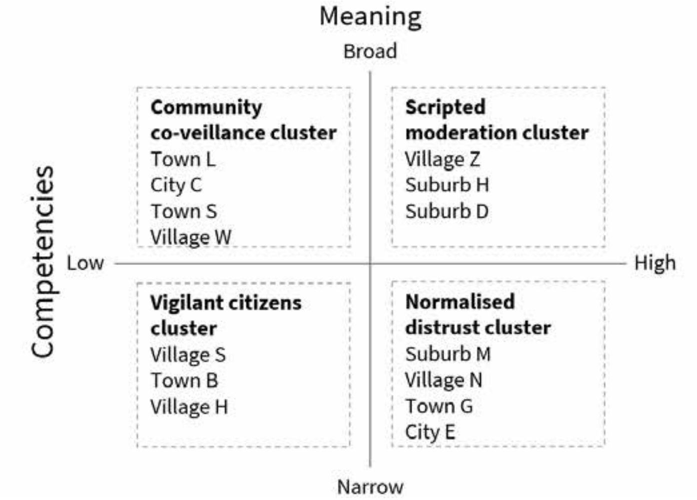
The competence dimension varies across groups because moderators differ in their access to professional knowledge and support. In some of the neighbourhoods, police and municipalities inform and advise the WhatsApp moderators actively (*high competencies*), whereas such knowledge is absent in other neighbourhoods (*low competencies*). In the interviews, the purpose of the groups was discussed, and it became clear that the meaning that members and moderators attribute to the practices they perform ranges from narrow to broad. In neighbourhoods where the WNCP group has a *narrow meaning*, the focus is solely on safety; on preventing break-ins and burglaries. In contrast, other moderators want their groups to serve a *broad purpose* and also allow social support practices (such as watching neighbourhood children and supporting neighbours in need).

Table 1 lists the differences in meaning and competence. Based on these differences, four clusters can be identified with similar levels of competence and meaning. Figure 3 visualises these clusters and displays tendencies which are used as analytical tools in the analysis. These clusters present the main themes identified during the inductive analysis of the interviews. Overarching characteristics (like *community co-veillance*) are connected to competence and meaning. In order to grasp how these WhatsApp groups function and how their different configurations impact people that are (unknowingly) involved in surveillance practices, the characteristics and particular issues of each cluster are examined next.

Table 1. Differences in Meaning and Competence levels across groups

WNCP group	**Meaning**	**Competencies**
City C	Broad	Low
Town L	Broad	Low
Town S	Broad	Low
Village W	Broad	Low
Village Z	Broad	High
Suburb H	Broad	High
Suburb D	Broad	Medium
Town B	Narrow	Low
Village S	Narrow	Low
Village H	Narrow	Low
Suburb M	Narrow	High
Village N	Narrow	High
City E	Narrow	High
Town G	Narrow	High

Figure 3. Clusters with similar competencies and meaning



1: Community co-veillance cluster

The first cluster includes neighbourhoods in both rural village environments and urban contexts and is characterised by broad meaning and low competencies. More specifically, the WNCP groups in this cluster serve a broad purpose with room for social support, and they are initiated and sustained without police or municipal involvement. Group members have knowledge about their community but lack strongly enforced guidelines or access to professional (police) knowledge. As Klara (moderator Town L) notes: *"I don't even know who our community police officer is".* Consequently, group members use intuition and common-sense beliefs to make decisions about what is to be considered suspicious or deviant behaviour and how to react. There is no formalised hierarchy present as the low-profile set-up often includes multiple moderators (ranging from two to six moderators) and power structures remain invisible.

The groups in this Community co-veillance cluster are largely self-governing and have a relatively small group size (30-150 members). Their informal nature is emphasised by the broad meaning members attribute to the groups. First and foremost, the WhatsApp groups are targeted towards increasing safety in the neighbourhood. Kai, moderator in Town S, states: *"I believe that it also provides sort of a sense of security"*. While preventing burglaries and break-ins is the primary purpose of the groups, they leave room for social exchanges and social support. For moderator Pauline (City C), their WNCP practices are characterised by communality: *"Our sense of community is stronger now".* This communality is accompanied by a sense of increased social support, neighbours help each other. Moderators and members shared examples of practical, functional, and supportive content, e.g., a key chain found on the sidewalk (Pauline, moderator City C) and two parakeets that broke loose (Bert, moderator Village W). Moderator Kai (Town S) adds: *"Last week someone lost his cat, that's fine you know, just post that in the group".* More tangible forms of social support can also be activated via WNCP groups, as moderator Klara (Town L) illustrates: *"We said that [points out of the window] there, someone had knee surgery, [we said] if your husband is working, you can send a message in the WNCP group, like: Hey, who can help me out?"*

However, social support easily turns into social control and WNCP group members experience the watchfulness of others on a daily basis. Lateral surveillance (Andrejevic, 2002), or co-veillance practices (Mann, 2016), lead neighbours to not only monitor the streets but also their neighbours. These practices are guided by a physical dimension, the act of watching one another in the street. Neighbours physically keep an eye out on the street while simultaneously monitoring their neighbours digitally, WhatsApp offers digital settings that allow users to check when a contact was last seen online and if they have read their message. In Klara's Town L, neighbours are alert and keep an eye on the neighbourhood children, but this also leads to: *"everyone knows at what time everyone goes to work".*

Notably, not all neighbours feel comfortable with being monitored by their neighbours, Moderator Pauline (City C) illustrates: "*It is not always pleasant, because it can really feel as if you are being watched, and to what extent is that good?"* Inevitably, Pauline tries to protect her personal space: *"Sometimes you will keep a bit of a distance, they are your neighbours, but eh… you do not have to be walking in and out all the time".* Similarly, Bert (moderator Village W) describes how he feels ambivalent about social support and social control: *"Look, it is good that people care about each other and look out for each other... But, well, it is good that people look around anyway, but I'm like, social control, keep it out of my house, they don't have to know everything about me".*

The Community co-veillance cluster shows how multi-dimensional informal surveillance practices impact personal lives and daily experiences of neighbours in their own house in their own neighbourhood. This is experienced as beneficial when neighbours keep an eye out for each other and offer social support, yet some respondents feel watched and prefer less social control. Lateral surveillance is both a curse and a blessing in these small and informal WNCP groups.

2: Scripted moderation cluster

As opposed to the Community co-veillance cluster with its informal moderation and small groups, the Scripted moderation cluster is characterised by intense moderation and relatively large group sizes. Founders of these groups appointed co-moderators to share administrative and monitoring responsibilities in order to effectively moderate the large populations (the groups typically include 250-350 members and cover a whole village or suburban area). Similar to the groups in the Community co-veillance cluster, the meaning of the watchfulness practices is not solely limited to burglary or break-ins, moderators also welcome notifications of missing children and other pressing issues. Yet, social support is not provided by these groups, since the scope and size of the groups makes them less personal and more detached from everyday issues.

Guidelines and rules play an important role in these groups. Most groups base their guidelines on the *SAAR method*, an abbreviation that stands for *Signaleer* (be aware and notice suspicious situations), *Alarmeer* (alert the police), *App* (inform the WNCP network), *Reageer* (react in a safe manner) (*Huisregels*, 2015, see also Chapter 4). The SAAR method, devised in City E and adopted by many WNCP groups, can be seen as *abstracted knowledge* that circulates between sites of enactment (Shove et al., 2012). In other words, competence transcends localised WNCP practices. Village E moderators translated their knowledge into the abstract SAAR method which was shared online and subsequently decoded and adopted in other neighbourhoods. In the Scripted moderation cluster, the use of the SAAR method and additional rules is informed and complemented by professional knowledge, as these groups are supported by community police officers who provide day-to-day advice. Community police officers streamline the (lateral) surveillance practices in these neighbourhoods by actively guiding the WNCP moderators and members.

What should be evident in this is that WNCP practices are piecemeal configurations, bringing together different types of (professional) knowledge and networks. Instead of using technologies specifically designed for watchfulness practices (such as the application Nextdoor), moderators and members make do with the resources at hand. This bricolage approach (Ciborra, 1992) includes tinkering with the messaging app itself as improvisation and adjustments occur on the part of both moderators and members. The piecemeal character of WNCP groups often leads to misunderstandings and tensions in the groups – tensions caused by members that share content deemed irrelevant or inappropriate by other members or moderators. John (Village Z) provides examples of irrelevant content shared in his group: *"The sidewalk for example. If it's wonky and uneven, that has to do with safety, but you should go to the municipality. Or a damaged streetlight, you shouldn't post that in the WhatsApp group".* Likewise, it is deemed irrelevant when members unnecessarily react to questions or notifications: *"Someone asks: 'Does someone know about…?', and then everyone replies with: 'No'. While if they would wait until one person says 'Yes', no-one else needs to respond"* (Lars, member Suburb H). Irrelevant content is often caused by people accidentally sending messages in the wrong WhatsApp conversation. Member James (Suburb H) also made a mistake: *"I wanted to WhatsApp my daughter that she had to come down for diner – she was in the attic. So, I type: 'dinner's ready'. But then WhatsApp restarted because of an update, and I thought it was ready to go, so I pressed 'Send'. And I looked… Oops, it's in the WNCP group".*

Misunderstanding and tension arise in WNCP groups because certain key scripts are at play in the Scripted moderation cluster. These scripts – particular visions of the world inscribed in an object or artefact implying a specific relationship between the object and surrounding actors (Akrich, 1992) – combine a variety of actors. These range from an Internet connection, a smartphone, multiple human users, and text-, photo-, sound-, emoticon-based messages. The inscribed user (Latour, 1992) of WhatsApp is expected to be capable of using a smartphone, installing the application, and connecting with contacts. The high penetration rate of WhatsApp in the Dutch market suggests that many people follow this script successfully. Research shows that WhatsApp is primarily used as a private platform for interactions with close ties (Karapanos et al., 2016; Waterloo et al., 2017). The informal nature of these interactions in combination with the speed and ease of the platform are not compatible with the serious nature of WhatsApp neighbourhood crime prevention. Scripts based on the SAAR guidelines clash with the scripts of WhatsApp. As the earlier mentioned examples show, this easily leads to friction in the functional environment of the WNCP group.

The effectiveness of WNCP can be thwarted by misguided reactions and mistakes, which lead to frustrations and conflicts among members and moderators. Failed scripts of WhatsApp as well as the tailor-made guidelines hinder everyday experiences in the WNCP groups. Moderators assemble dispersed networks of neighbours, smartphones, WhatsApp software, streets, and houses in order to protect their neighbourhood and private space against actors with bad intentions. In order to make neighbours uniformly participate in neighbourhood surveillance practices, the moderators in the Scripted moderation cluster wrote (sometimes extensive) manuals. However, in almost all WNCP groups, frustrations and conflicts emerge when members fail to follow these manuals and thus, fail to adhere to the scripted practices.

3: Vigilant citizens cluster

This cluster of small-scale WhatsApp groups (30-70 members) is characterised by vigilant behaviour in order to prevent break-ins. In contrast to the previous two clusters, the groups within the Vigilant citizens cluster attribute a narrow meaning to their practices. The group moderators do not allow practical or social matters to be discussed in the WNCP group. Moderator Louise (Village S) even decided to create an additional group to solve tensions similar to the aforementioned discussions about irrelevant content: *"For all the other things that people deem important, we made a social app group".* Notably, the existence of a social group is an exception but emphasises the strict and focused character of the WNCP groups in the Vigilant citizens cluster: *"The app is purely meant for fire, break-ins and real emergencies"* (Louise, moderator Village S). The neighbours within the groups of this cluster display a vigilant mind-set and voluntarily engage in surveillance practices. Notably, they go further than the participants in other WNCP group clusters because they actively started to police their neighbourhood. The specific configuration of dimensions in this cluster can be characterised by narrow meaning and low competence levels because no police actors have been involved in initiating or moderating the groups. The vigilant surveillance practices in this cluster are a precarious form of participatory policing (Larsson, 2017).

Citizen initiated policing activities can affect passers-by who are (often unknowingly) subject of watchfulness practices. When walking through an unfamiliar neighbourhood, there is always the chance of being watched by residents. While spying eyes and suspicious glances might make one feel uncomfortable, WNCP surveillance practices augment this. Suspicions about passers-by are immediately materialised when a WNCP member sends a WhatsApp message to neighbours. This can lead to more neighbours peering through blinds or pulling back the curtains, which will invariably affect the experiences of passers-by. Furthermore, it is not just messaging but also the potential to be photographed. Cameras on smartphones can be used in unnoticeable ways and a picture of an allegedly suspicious person can be snapped in a split second. WNCP members often share images, and some go great lengths to collect visual proof. Harold provides an example:

> *"My wife said: 'what a strange man, he walked by and stopped to look at the houses', so I jumped on my bike to see where he went...And I held my smart phone camera in front of me, and took a picture of him. And these pictures I sent to the police. He didn't notice at all that I was taking a picture of him."* (Harold, moderator Village H)

Photographing strangers and sharing pictures with police creates significant privacy concerns. These infringements are even bigger when smartphone pictures and surveillance camera footage are shared within

WNCP groups. People who are photographed do not even have to raise suspicion. Not knowing someone can be reason enough to directly materialise even the smallest cause for doubt or distrust, i.e., to take a picture and share it in the WNCP group. However, not all moderators advocate this type of active behaviour. Some of them only allow pictures of people who are acting obviously suspicious or, as moderator Sven (Town B) explains: *"Not until you clearly see that someone walks into gardens, looks into windows and is checking the gates".* Likewise, an often-used rule is one that permits sharing of pictures within but prohibits the distribution of pictures outside of the WNCP group. However, the ease with which visual digital material can be distributed within and beyond WNCP groups presents privacy issues for all actors involved.

Whereas the moderators have communicated guidelines when they started the groups, these rules are often not strongly enforced. Events in Village H show that a low level of competence can cause risky situations. This group stands out because it is the most active group in the sample. During the moderator interview and the focus group with members, it became clear that a relatively large number of warnings is exchanged in the group. At least once a week one of the neighbours notifies the group about an allegedly suspicious situation, break-in, or another event. Most groups are used far less often. Moreover, moderators and members of Village H frequently take immediate action when they receive a notification.

The abovementioned SAAR method is customarily ignored in highly vigilant neighbourhoods like Village H. Instead of informing the police before taking action, these citizens directly, and often impulsively, react to alerts. Member Vera (Village H) provides an example of a recent event when she distrusted a van that was parked in her street *"...So my husband went to the car, and just said: 'Can I help you, is there something wrong with your car?' At that time another person came up, that jumped into the van, and they were gone".* Vera reported the suspicious van in the WhatsApp group while her husband confronted the driver, but she did not contact the police until after the van left. In this and similar situations, the neighbours put themselves at risk. Interactions with suspicious persons might get out of hand or groups of members can get carried away in the heat of the moment. Vigilant actions of neighbours might be aimed at preventing break-ins, some neighbours simultaneously enjoy their participatory policing practices. Members Theo states: *"It is just exciting (...) Life is one big risk".* This excitement leads to behaviour that can put members and allegedly suspicious persons at risk.

Additionally, surveillance practices are likely to lead to widespread suspicion and ambivalence between neighbours (Reeves, 2012). In Village H, this became evident when moderator Betty saw a person running past her house at the beginning of the evening, a man wearing black clothes and a beanie. Betty did not trust the situation and got into her car: "*So I drove around to see where that man went. And later, I posted it on the WNCP group, and then I received a message: 'Yes, that is the husband of one of the women in the WhatsApp group'".*

This example shows that vigilant surveillance practices can default to the lateral surveillance of neighbours not only in the form of monitoring but also by actively following them. Notably, whereas the activity and eagerness to take action are relatively high in Village H, this behaviour, the resulting suspicion, and risks are not limited to this neighbourhood. Multiple moderators shared stories of members that experience messages in the WhatsApp group as a direct call to action. This particularly concerning configuration of practices results in vigilant behaviour which blurs the boundaries between police and citizen responsibilities and puts neighbours and allegedly suspicious persons at risk. Chapter 4 provides a more in-depth analysis of vigilant behaviour in WNCP groups.

4: Normalised distrust cluster

The Normalised distrust cluster includes four large groups with a narrow purpose focused on preventing break-ins, which stand out in their high level of competence visible in a level of professionalisation. In all four groups, community police officers were closely involved in the initiation, promotion, and construction of the groups and thus set the tone for these practices. Police officers assisted in the design of guidelines and are connected to the moderators in a separate WhatsApp group in order to support them and to use the group's assistance during police actions. Furthermore, the moderators monitor multiple WhatsApp groups that function in compatible manner. Each group covers part of the area and is monitored by a local moderator (on street level) while the interview respondents, who can be seen as supra-moderators, hold an oversight position. Ron describes the design of his groups:

> *"We have nine WhatsApp groups which are named after their streets, and above these groups is another group and that is the Chief Control group. And in that group are, as I named them, the Ambassadors (...) and they are all part of that Chief Control group, but they are also the moderators of their own WhatsApp group. Let say that, in group [street name] there is a notification. I see that notification and I post it in the Chief Control group. All Ambassadors will see the notification and they take it up and forward it to their own WhatsApp group. This way, we can inform the whole village in three minutes."* (Ron, Village N)

These professionalised groups are strictly moderated and comprise formalised practice bundles (Shove et al., 2012). The configuration of these combined efforts is documented in manuals and whereas they are constructed independently, these practice bundles coincide with municipality and police practices. The self-imposed power that supra-moderators provide themselves with creates a distinct hierarchy in neighbourhood networks. The functioning of multiple WNCP groups in a neighbourhood is controlled by one or two individuals who have created this position for themselves. The large-scale nature of these groups (300-3000 members) increases the impact of neighbours' everyday surveillance activities and presents similar issues as in the other clusters but on a larger scale. The rules and conventions of WNCP groups are still in development while they are simultaneously normalised.

When participating in these large-scale WNCP groups, neighbours become acutely aware of particular events which alters their experience of the neighbourhood. Activities in the street that previously would have gone unnoticed, are now materialised into WhatsApp group messages. Neighbours actively monitor their neighbourhood and share suspicions; they also work together in information searching practices (such as looking up a license plate registration online). WNCP participation sensitises them to suspicious activities. A hitherto underexposed pressing concern of these practices is how determining what is seen as suspicious leads to the normalisation of categorisations and wrongful accusations. When neighbours engage in surveillance practices, they scan the street and assesses the situation at hand. This assessment is based on competence and meaning. The knowledge consulted when making a distinction between suspicious and non-suspicious persons and behaviour is guided by a categorisation of normal and deviant activities. Nevertheless, conventions about what counts as suspicious or deviant behaviour are ambiguous, there are no clear categories of normal/suspicious/deviant behaviour and persons.

In the interviews it became evident that the categories used by neighbours are often based on stereotypes and prejudice. A worrying number of incidents reported in all four clusters revolved around wrongful accusations based on intolerant categorisations. An example of a situation like this became visible in Suburb H (in the Scripted moderation cluster), where a neighbour consulted the group to voice concerns about a couple of men sitting in a car with a Polish license plate. Henry (member) recalls: *"And then immediately someone replied: 'Yes, they belong here, they live here'". Dave (member) explains: "They were only waiting for someone to get in the car".* This anecdote and similar cases show that intolerant categorisations are normalised in many WNCP groups. In the large groups in the Normalised distrust cluster, the scale of these discriminatory practices increases, and adequate responses of moderators and involved police seem to remain absent. The fact that these groups widely promote their WNCP templates and methods without addressing these issues, leads to the conclusion that the normalisation of surveillance in WNCP practices includes a concerning normalisation of suspicion, distrust, and intolerance towards strangers as well as neighbours (Reeves 2012; Larsson 2017).

Conclusion: Amplified (lateral) surveillance practices

WhatsApp proved to be a technical layer in the amplification of surveillance practices guided by materialised suspicions. The implementation of WhatsApp into watchfulness practices changed neighbourhood dynamics and personal experiences. The existence of a WNCP group alters how neighbours experience their street because concerns and possible threats become more immanent. This urges many neighbours to take up their responsibility and contribute to surveillance practices in order to safeguard their neighbourhood. These practices are co-constructed as they are the result of collaborative efforts of neighbours, sometimes in conjunction with police or municipality actors. The immense popularity of this recently emerged phenomenon is of ambivalent nature and has precarious consequences. This chapter showed that while citizen participation in crime prevention leads to an increase in social support, feelings of safety, and the active prevention of break-ins, it is also **accompanied by risky acts of vigilant behaviour**. Furthermore, the monitoring of passers-by defaults to lateral surveillance practices, which **impacts the individual experience of citizens in their own homes and streets**. The inscribed user of WhatsApp is often not compatible with the inscribed WNCP member that moderators have in mind. Caveats between scripts and daily practices lead to friction among neighbours.

The focus on WNCP practices enables an examination of lateral surveillance as a combination of digital and physical practices, a valuable contribution to existing literature focusing on digital lateral surveillance practices (Andrejevic, 2002, 2007; Lee et al., 2017; Trottier, 2012). Particular *"suspicion-driven rituals of lateral surveillance"* (Reeves, 2012, p. 238) are initiated by citizens which causes risky behaviour and intolerant attitudes to be normalised and integrated in community life. The standardisation of these practices needs to be critically assessed, not only by social scientists but also by institutional actors involved such as municipal policy makers and police officers. Namely, these vigilant communities in the making raise significant issues for communities, police and municipalities and the transition of practice bundles across neighbourhoods raises questions about adjustments and standardisation processes.

Whereas this chapter is limited to an in-depth snapshot of particular Dutch practices, issues were identified that mirror the risky consequences of participatory policing practices in institutionally initiated practices in countries such as the US. The use of a practice theory lens proved to be particularly helpful in distilling the general issues of citizen participation in WNCP surveillance practices. The WNCP group clusters that I identified were crucial in uncovering a variety of pressing issues arising from inherently diverse WNCP practices. This chapter shows that the emergence of WhatsApp amplified all three dimensions of a variety of neighbourhood watchfulness practices still in the process of stabilisation and normalisation.

Limitations and suggestions for future research

This chapter explores the topic of WNCP practices and aims to provide a concise yet comprehensive overview of the benefits and drawbacks these practices bring, with a particular focus on lateral surveillance. Power is a key concept that is only touched upon briefly in the results section yet deserves more attention in future research. In WNCP as well as in similar neighbourhood watchfulness practices, power inequalities arise between active and engaged participants and unknowingly involved citizens. Moreover, an imbalance in information can arise because it too often remains unclear which actors have access to which information – e.g., in practices where police officers are involved. The question arises how this produces an arrangement of relationships within neighbourhood contexts, with commercial, law enforcement and citizen actors with unequal power structures and non-transparent information sharing.

Moreover, I focus on WNCP practices in the Netherlands, and while the sample is diverse, the practices are immersed in and influenced by the local context and culture. For future research, it would be good to see how the interplay between meaning, competence and material dimensions differs or is similar in WhatsApp watchfulness practices in other countries[4]. For example, neighbourhood block watch groups in the UK, South Africa, and Australia also use WhatsApp for crime prevention. Even though these initiatives are not as widespread as they are in the Netherlands, they might be dealing with similar issues as outlined in this study. Future research should look into how cultural backgrounds influence neighbourhood watchfulness practices and how different contexts create different meaning and competence dimensions in these practices.

[4] Examples of WNCP practices across the world: UK: https://www.guardian-series.co.uk/news/16108413.neighbourhood-watch-use-whatsapp-to-stop-crime, South Africa: https://gbnw.co.za/whatsapp-sign-up/, Australia: https://www.abc.net.au/news/2019-02-02/neighbourhood-watch-these-days-are-all-about--whatsapp/10763624

In addition, especially in the US, commercial platforms have introduced similar networks which citizens can use to collaboratively safeguard their neighbourhoods. Nextdoor, a social networking platform for neighbours, includes a section on safety wherein law enforcement and municipalities can take part ('Nextdoor Public Agency', n.d.). And recently Amazon introduced Neighbours, an app wherein citizens can exchange photos and videos of their smart doorbells in order to notify their neighbours of suspicious activities on their streets ('Press Kit', n.d.). Similar to Nextdoor, law enforcement can take part in these networks. The integration of law enforcement not only raises concerns about the privacy of alleged 'suspects' whose images are shared on the app without their knowledge, but the commercial basis of these platforms also amplifies these concerns. Because the commercial nature of these apps creates another dimension to watchfulness practice, a dimension that brings up urgent questions about data collection, and ownership of the images and videos shared on these platforms.

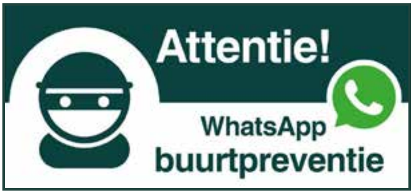
Chapter 4

"A sense of security" Participatory policing in WhatsApp neighbourhood crime prevention groups[5]

Introduction

When walking the streets of Dutch suburbs and villages, it is likely to come across a number of similar sights. Cars are parked along clean streets and often small trees are planted every ten metres near sidewalks made of brick pavers. Blocks of identical linked houses with small well-kempt front yards have open curtains that enable a glimpse of the interiors and homey scenes. Additionally, in many neighbourhoods there are official looking street signs which display a WhatsApp-logo and the text: *"Attentie! WhatsApp Buurtpreventie"* (translation: Attention! WhatsApp neighbourhood crime prevention). Many of these signs include a villain-like icon and a reference to the website https://wabp.nl, see Figure 4. These signs alert the viewer that neighbours within this area are connected via WNCP groups focused on neighbourhood safety and crime. It is a visible marker of an otherwise mostly invisible participatory surveillance network.

Figure 4. WNCP sticker that was available via https://wapb.nl in 2018



[5] This chapter is a slightly altered version of: Mols, A., & Pridmore, J. (2019). When Citizens Are "Actually Doing Police Work": The Blurring of Boundaries in WhatsApp Neighbourhood Crime Prevention Groups in The Netherlands. *Surveillance & Society, 17*(3/4), 272–287.

The arrival of WNCP groups in the Netherlands (see the introductory chapter for an explanation including an overview of the benefits and drawbacks) signals a shift in relations between ordinary citizens and policing practices. This chapter explores everyday practices within WNCP groups, which vary from self-organised, citizen led, DIY policing practices to police-initiated surveillance projects (Chapter 3 provides an overview of different types of WNCP groups). WNCP practices can be seen as a form of participatory policing because citizens actively assist law enforcement (Larsson, 2017).

While the role of these groups as a form of participatory policing is still in the process of stabilising, WNCP groups can be seen as heterogeneous local surveillance networks that provide for the potential to collaborate with police or create semi-autonomous citizen policing practices. Most WNCP groups (all groups in our sample) use the *SAAR-guidelines* promoted by https://wapb.nl. These guidelines are developed in one of the WNCP groups in our sample. In 2013, when the first WNCP groups emerged, two community police officers and one moderator in City E came up with the abbreviation SAAR, which stands for:

> *“Signaleren: Be aware and notice suspicious situations*
> *Alarmeren: Alert the police*
> *App: Inform the WNCP network via WhatsApp*
> *Reageren: React in a safe manner – e.g., by approaching the suspicious person”* (‘Huisregels’, 2015)

These guidelines can be seen as an attempt to normalise the use of WNCP groups as it provides a template that can be duplicated in other neighbourhoods. We pose the question: **How do participatory policing practices in WNCP networks relate to the advised SAAR guidelines?** This chapter shows that upon closer examination, the actual and often invisible uses of WNCP groups diverge from the intended process in the SAAR-guidelines.

In what follows, we discuss how WNCP practices can be understood in light of current research about participatory policing and its consequences. Afterwards we turn to discussing, in relation to each step of the SAAR method, how these guidelines have been interpreted and improvised in actual practices by members of these groups. Our findings demonstrate that the everyday use of WNCP groups complicates the ways in which citizens make their own neighbourhoods *safer* in collaboration with the police. These complications have to do with shifts in power dynamics between citizens and police and how the use of such groups increases the *responsiblisation* of citizens for their own safety, something which can be seen to both aid and interfere with police practices and investigations. This fits with a broader global neo-liberal trend of citizen responsibilisation which critiques the *off-loading* of responsibilities from formal political institutions such as the police onto citizens, creating responsible individuals in self-governing communities (Rose, 1996; Yesil, 2006).

We argue that the responsibilisation of citizens in WNCP groups and the way their everyday practices divert from the intended process default to more problematic forms of participatory policing, including increasing discriminatory practices, normalising suspicion, risky vigilantism, and issues of accountability. Importantly, this type of participation amplifies concerns about both racially biased police practices and xenophobic citizen perspectives and the effects these have on marginal populations in The Netherlands. By incorporating forms of citizen-initiated participatory policing, this chapter adds a new and interconnected dimension to prior research about participatory policing. As such, our focus on citizen-led participatory surveillance differs from existing literature which tends to emphasise government-initiated campaigns.

This in-depth account of local processes of citizen responsibilisation builds on interviews with citizens and police officers involved in WNCP. We provide insights in police-citizen interaction in a country where community policing practices are more and more pervaded by digital and physical citizen initiatives. We demonstrate that these WNCP groups are both an innovative and problematic development and highlight a number of tensions that arise between the more visible and invisible aspects of these participatory policing practices.

Literature: Community policing and participatory policing

In order to contextualise WNCP practices, this section describes how they take place in the context of community policing. Afterwards, participatory policing and responsibilisation are discussed as the core concepts needed to understand citizen-initiated policing practices.

WNCP networks in the context of community policing

In order to examine the relations between WNCP groups and police, this chapter draws on interviews with citizens and police across twenty neighbourhoods in The Netherlands. All neighbourhoods are monitored by Dutch police as part of their core tasks, described as maintaining public order, investigating criminal offences, providing assistance in emergencies, and identifying safety and security problems (Toorman & Den Engelsman, 2009). The Dutch police organisation is divided into national, regional, and local levels.

On the local level, the police are specifically responsible for ensuring a safe and liveable neighbourhood and city (‘Politietaken’, n.d.). In this context, community police officers are increasingly seen as important actors. The Dutch police organisation strives to have one community police officer for every 5000 citizens. Community police officers have an awareness, advisory and directive role in neighbourhoods, mainly targeted towards social issues, minor crimes, environment, and traffic (‘Wijkagent’, n.d.). One of the interview respondents describes his work as a community police officer as follows:

> *“A community police officer is expected to know what’s going on in the neighbourhood, to be visible in the neighbourhood, and to be in contact with the business owners, residents, and with professionals working in the neighbourhood…It’s not only the social but also the repressive [restrictive approach]… Like, is there a specific approach to youth groups needed? Then you need to know who hangs out where and what they’re doing. And apart from that, there are many different reports. If there’s a report in the neighbourhood about noise or domestic violence, then you’re expected to go there, to check what’s happening.”* (Bart, community police officer)

These reports and the awareness of problems and nuisances at a local level are central to this chapter. We look at how citizens connect and collaborate with community police officers in WNCP networks as well as how they independently carry out policing practices. Citizens increasingly engaging in monitoring, information sharing, and crime-disrupting practices is a form of participatory policing through these messaging groups.

Participatory policing and responsibilisation

As suggested by Larsson (2017), participatory policing entails citizens actively assisting law enforcement by engaging in monitoring, information-sharing, reporting, and preventative actions. The emergence of participatory policing highlights a transition in policing methods. In previous decades, everyday engagement in policing changed from a focus on apprehending criminals towards one of prevention and problem solving. This later focus involved non-police actors in various ways, ranging from private security firms to active citizens (Shearing, 1994). Citizens were seen as social actors who can aid police and make the social control process more effective by being aware of suspicious behaviour in their neighbourhood and by showing *“a readiness to report incidents to the police and to co-operate”* (Avery 1981, 76). Moreover, the emergence of community policing as part of a preventative transition in part enabled a change in defining police as a *force* towards police as a *service* in which policing becomes in fact *“everybody’s business”* (Shearing, 1994, p. 8).

Most research about participatory policing has focused on law enforcement-initiated campaigns, such as nationwide vigilance campaigns in the United States, Canada, United Kingdom, and Australia. Research about local projects and campaigns focuses on community police-led participatory policing practices (Ryan, 2008; Shearing, 1994; Varghese, 2009; Walker & Walker, 1990). These local participatory policing projects are based on pro-active co-operation between citizens and community police (Walker & Walker, 1990).

In contrast, nationwide public vigilance campaigns have a top-down structure; law enforcement requests participatory policing in the form of being aware of particular (signs of) threats and criminal or terrorist activity (Larsson, 2017). Subsequently, citizens are asked to share their suspicions via *anti-terrorist hot lines*, online reporting forms, text messaging services, and smartphone applications (Larsson, 2017). Many of these campaigns emerged after September 11, 2001, and have names like *If You See Something, Say Something* and *If You Suspect It, Report It* (Larsen & Piché, 2010; Larsson, 2017; Reeves, 2012). These public participatory surveillance campaigns “*involve the many watching the many on behalf of the few” (*Larsen & Piché, 2010, p. 196). For this chapter, one of the key differences between the participatory policing projects described above and WNCP groups is their origin. Whereas public vigilance campaigns have been largely initiated by institutions or governments, this form of participatory policing emerged in a grass-roots fashion. WNCP groups are by and large citizen-initiated, organised, and led. While this chapter includes both police- and citizen-initiated participatory policing practices, our analysis shows how these different configurations bring specific challenges and power structures.

Increasingly forms of participatory policing have become predicated on the use of new technologies as suggested by Larsson (2017). Whether this involves the use of the telephones to call emergency numbers, the use of online reporting forms, or the more recent use of specific apps, technology has become a crucial component in the modern variations of both the *see something, say something* campaigns as well as in WNCP groups. In theory, smartphone applications and social media channels make participatory surveillance practices accessible to all citizens (Larsson, 2017). There is a low threshold to communicate information for members of WNCP groups because they make use of messaging applications that are freely available and already in use. Unlike the *if you see something, say something* numbers to call or text in suspicious activities which are used for public participatory policing campaigns, the messages within these messaging apps are not monitored or owned by government institutions. Instead, they are owned by commercial institutions (WhatsApp is part of Facebook) and the conversations play out in (to a large extent) an invisible and uncontrolled environment (Sutikno et al., 2016).

Despite this invisibility and limited control, such forms of public vigilance to observe and report concerns can be seen as a way to identify threats, prevent criminality and reduce certain pressures on police. Yet these also can become the default in normalising policing practices, potentially creating and increasing forms of social distrust. It is inevitable that participatory policing practices, initiated by either law enforcement or citizens, make citizens more aware of potential criminal activity in their community and sensitises them to security threats that may be perceived of as real regardless of whether there is imminent danger. This orientation to one’s surroundings and engagement in participatory policing practices has become normalised and *“many citizens have assimilated into their everyday lives suspicion-driven rituals of lateral surveillance”* (Reeves 2012, p. 238). In the process, citizens become surveillance agents whose distrust towards strangers and suspicion and ambivalence among neighbours is increasingly perpetuated (Larsen and Piché 2010; Larsson 2017; Reeves 2012). A specific way of life is normalised, in which unwanted persons can be identified and specific appearances and behaviour will be seen as suspicious (Larsson 2017).

These public vigilance campaigns are about encouraging citizens to assist law enforcement in surveillance activities – participatory surveillance practices based on forms of lateral surveillance; peer-to-peer monitoring *“of spouses, friends, and relatives”* (Andrejevic, 2002, p. 481). The introductory chapter and Chapter 3 show that, in contrast to the more often described forms of digital lateral surveillance, lateral surveillance in public vigilance campaigns has important non-digital components. As such, our understanding of lateral surveillance includes digital as well as non-digital peer-to-peer monitoring practices. This means that alongside everyday digital connections such as on social media, citizens watch one another in person and spend time checking their environment and the behaviour of other citizens in that space. Chan (2008) argues that lateral surveillance as requested by (trans)national public vigilance campaigns create and induce a culture of suspicion driven by vigilance and constant suspicion – this is seen to easily diverge into a culture of hatred, characterised by racial stereotyping, discrimination and harassment.

This chapter reiterates that crime prevention campaigns are geared towards the responsibilisation of citizens (Chan, 2008; Reeves, 2012), and that these new forms of participatory surveillance prompt citizens to take responsibility for their own neighbourhood safety (Purenne & Palierse, 2016). Not only are citizens mobilised to monitor their environment in order to identify and assess risks for crime and terrorism prevention purposes, but they are made responsible for *“policing their own territory”* (Haggerty & Ericson, 2000, p. 156). Thus, they are not only expected to monitor their neighbourhood, but also to actively safeguard it. Responsibilisation of citizens can be understood as the precarious transition of law enforcement responsibilities to community members.

In this case, WNCP entails a voluntary and citizen-initiated form of citizen responsibilisation.

However, while voluntary, as Sandhu and Haggerty (2015) suggest, citizens are actively stimulated to take this greater responsibility within their communities to manage (potential) security risks. Arguably they internalise law enforcement strategies and use these in their own community (Andrejevic, 2002). Consequently, citizens become responsible for the safety and security of not only themselves, but their communities and fellow citizens (Reeves 2012). In many participatory policing projects, it is implied that failure to be vigilant is risky and irresponsible (Larsen and Piché 2010) and this implicitly accuses citizens who refuse to participate as obstructing processes of safeguarding the neighbourhood. Crucially, this responsibilisation blurs the boundaries between police, citizens and suspects and makes more ambiguous the role of the actors involved in participatory policing practices (Reeves 2012). By contrasting the SAAR guidelines with the actual practices of our interviewees, this chapter highlights the precarious consequences of responsibilisation within WNCP groups for different actors in these diverse configurations.

Research method: WNCP interviews and focus groups

This chapter is based on interviews and focus groups with 27 moderators and members by us and 13 additional interviews conducted by a master's student. Methodological details are included in Chapter 2, the interview guide in Appendix 5, and the respondent overview in Appendix 1 gives an indication of the type of neighbourhood they live in and provides information about the involvement of police in their groups. The results of the three-stage constructivist grounded theory procedure (Charmaz, 2014; Corbin & Strauss, 1990) are included in the codebook in Appendix 11 and detailed in the next section.

Results: The gap between guidelines and WNCP practices

As noted, the WNCP groups studied are heterogeneous networks of citizens, smartphones, and police actors, in some cases further supplemented by other municipal actors. Even when WNCP groups are not initiated or (in)directly supported by police, citizen practices targeted towards neighbourhood safety are always connected into the domain of policing more broadly. While WNCP practices may not yet be fully stabilised, we argue that they can be seen to be in a (somewhat problematic) process of normalisation. As more and more communities introduce WNCP, the practices of existing groups are used as a template and are increasingly becoming the norm for how a WNCP group should and must operate. This is still not universal, however a key factor in this process has been the implementation of uniform guidelines across these groups. It was one of the neighbourhoods in our sample that came up with the set of rules indicated above using the acronym *SAAR*, which is used in almost all WNCP groups and forms the *house rules* for participation indicated by the primary WNCP website ('Huisregels', 2015). Though it is not clear to what degree the average user is familiar with these guidelines, SAAR has been recommended by the national Dutch police.

In what follows, we use the terms of the SAAR approach and focus on how these instructions can be seen to relate to actual practices. From our research, it is evident that practices often diverge from the intended processes, which leads to various internal and external tensions. These tensions are related to a process of responsibilisation, which obscures the differentiated formal and informal roles of actors within WNCP networks (Reeves 2012). Based on SAAR, our results carefully compare intentions to actual practice which lead to some precarious consequences for this form of participatory policing.

Signaleren: Be aware and notice suspicious behaviour

The SAAR method starts with an instruction that does not require direct action. Instead, the method demands a state of constant awareness and attentiveness from WNCP group members. Neighbours can participate in safeguarding their neighbourhood by keeping an eye out and by carefully watching their street. As citizens engage in participatory surveillance practices when they actively monitor their environment, they become increasingly responsible for the safety of their neighbourhood. Moderator Ron explains why neighbours can play a crucial role in moderating practices: *"As neighbours we can see the difference between a resident and a stranger. For them [the police] everyone is unfamiliar; they have to use their intuition while we have the facts".* Community police officer Ron further describes how he and his colleagues direct these participatory surveillance practices through the WhatsApp group: "*You can focus this on a specific area: 'pay attention to this' or 'look out for a particular car'. And people can notify you what they directly see".* As in these cases, police officers are making active use of the *responsible* citizens' monitoring practices.

However, these monitoring practices are based on a somewhat problematic premise: monitoring suspicious activities in the neighbourhood defaults to monitoring neighbours. As people become constantly alert and scan their neighbourhood for suspicious behaviour or for security and criminal problems, this behaviour reinforces lateral surveillance practices. For instance, group member Theo describes the routines of his neighbours: *"I know quite a few [neighbours] that, with their dog, walk through the whole neighbourhood. They do this every night around eleven, eleven thirty, because, my garden lights will switch on and I see them passing by".* Though Theo's monitoring practices are not directly targeted at neighbours, they give him insight in their behavioural patterns. Group moderator Marc actively monitors his neighbourhood and purposefully checks up on his neighbours:

> *"Often, I walk around the neighbourhood once or twice a week, because it is healthy, but also because I am the [WNCP group] moderator, I just make a round. And then you'll see, I kind of check what's going on. People keep their curtains open at night, which is special, but you'll directly see if the right people are on the couch or not."* (Marc, WNCP group moderator)

The fact that Marc checks if the *right people* are on the couch is predicated on him presumably knowing whom the right and wrong persons might be. It seems his evening walks are less motivated by his health and enjoying his neighbourhood, and more by the desire to check if something is wrong in the neighbourhood. This impetus towards monitoring is visible in most WNCP practices. Notably, Marc has made himself increasingly responsible for checking his neighbourhood.

Both Marc and Theo's practices show how being watchful for neighbourhood safety can easily lead to monitoring the daily behaviour and patterns of neighbours. Even though citizen-member Bram says that the alertness of his neighbours *"gives me a feeling of safety",* not all neighbours feel comfortable with these practices. A moderator of one of the WNCP groups, Bert, describes his own ambivalent feelings: *"It is good that people keep an eye out, but eh, I'm always a bit, well, [concerned about] social control...Not in a positive manner, they just don't have to know everything about me".* Notably, whereas Bert and other WNCP group members are aware that they might be monitored by their neighbours, this form of lateral surveillance includes an uneven balance between members and non-members of the groups. Most non-members are unaware of when and how they might be target of surveillance by their neighbours, specifically because they are not included in conversations about monitoring experiences and results. The use of a WhatsApp group for *signaleren,* which, although the Dutch word hints at signaling suspicious activity, is really focused on awareness and attentiveness, leads to a neighbourhood where lateral surveillance becomes the status quo. This intensifies the in/out group dichotomy at a local level, with suspicion and distrust towards strangers and neighbours increasingly a default view. Though conceived of as a means of engaging neighbours in securing their own neighbourhoods, these responsibilisation practices begin to normalise a culture of suspicion within these groups (Chan 2008).

Alarmeren: Alert the police

When WNCP group members come across situations they deem suspicious, they are instructed to first alert the police. This is supposed to happen before they inform the WNCP network or take any action. The police can then assess the situation and provide instructions for the group. However, our interviews show that WNCP group members often skip this step because they are hesitant to call the police. They would rather inform their neighbours first. WNCP group moderator Marion describes her hesitation:

> *"The first time it was kind of a hurdle. You think: 'should I call, or shouldn't I?' You start to doubt your own feelings, what if you, eh, put the blame on an innocent person? ...And the first time, it turned out to be nothing, but still I received feedback from the police officer, like, 'Yes, good that you notified us'."* (Marion, moderator WNCP group)

In practice, within many groups, the WNCP network is alerted before the police are informed. This means that suspicions are first directly made visible to large groups of people. In principle the SAAR guidelines enforce a shared responsibility between citizens and police to take appropriate steps when suspicious behaviour occurs. Though, when WNCP members fail to notify the police first, they make themselves and their fellow WNCP group members automatically responsible. This raises questions of accountability early in the process. Who is held accountable for the outcome of actions to deal with suspicious situations?

The idealised SAAR model prescribes that citizens only need to voice suspicions based on actual behaviour, yet in practice it is difficult for citizens to determine what constitutes suspicious behaviour. Several interviewees indicated that their suspicions are constructed on the basis of particular characteristics instead of behaviour. Many people, interactions, and cars will not be seen as suspicious, while particular persons are directly mistrusted. As noted by Larsson, *“only certain appearances and behavioural patterns will become reported as ‘out of the ordinary’, and individuals behind this veil of distrust will indeed have a hard time ‘participating’ in securing anything once they become deemed potential threats”* (2017, p. 98).

The particular characteristics employed in making suspicious persons or situations visible in WNCP groups often have to do with any deviation from the unexpressed norms. Bert, group moderator, explains one situation: *“A while ago, a car with a foreign license plate drove by, and stopped at multiple corners of the street. So then, the police were called”.* Other examples in the interviews revolved around people with a Polish, Moroccan or Turkish license plate or nationality, or a specific skin colour, characteristics that align with marginalised groups in The Netherlands. The two following examples about allegedly suspicious persons with a Turkish nationality show that suspicion and distrust are based on appearance:

> *“She [a neighbour] accused someone: ‘Hey that is a suspicious person who is not okay.’ Unfortunately, that was the Turkish, window cleaner that comes here often...At a certain point she posted a picture of him, and then someone said: ‘Whoa! That man has been coming to my house for years!’”* (Bert, group moderator)

> *“That happened one time in the WNCP group. Someone said: ‘there was a suspicious car, the door was open for a long time, but they were chatting, and when I looked in their direction, they immediately left’. And then a girl reacted angrily: ‘What the hell! That was my boyfriend and we were chatting. Why is he suspicious? Because he is Turkish?’ That sort of things happens, you know.”* (Saskia, moderator)

These discriminatory practices show a deep distrust towards particular societal groups. On many occasions, WNCP group action is structured by particular categories deriving from a fear of an ambiguous *other*. Many WNCP groups have deeply problematic views on suspicious activities and persons, mirroring discriminatory practices for which the police are often accused. As Haggerty (2012) notes, citizens may replicate police practices which (possibly unintentionally) categorise people and selectively discriminate against the persons and behaviours of people within specific groups. *“Selective monitoring often gives rise to accusations that the police are discriminatory; that police surveillance is being used to control and criminalise certain groups”* (Haggerty, 2012, p. 236). While the overall intentions of most WNCP group members may not be by default discriminatory, both intentional and unintentional discriminatory monitoring practices of these groups are even more invisible than bias by police.

Of course, a number of Dutch community police officers are involved in WNCP groups. Concerns about discriminatory practices in WNCP groups are amplified by the fact that, as an organisation, the Dutch police have been accused of ethnic profiling a number of times (Çankaya, 2015; Van der Leun & Van der Woude, 2011). For the most part, ethnic profiling practices have been primarily directed towards migrants or, more specifically, people with a Turkish, Moroccan, West-African, Antillean or Eastern-European background (e.g., see the examples offered by Çankaya, 2015). Though these concerns are not new, having been prevalent for years (e.g., see Esmeijer & Luning, 1978), the possibility that these discriminatory perspectives may be integrated into WNCP networks which themselves have limited diversity, creates a potentially volatile situation. Arguably the police have an important role in enforcing cultural-normative order and should be active in uniting disparate communities (Çankaya 2015), but it is unclear that this is happening within these contexts. As WNCP groups often show similar problems on a smaller scale, certain neighbourhoods become increasingly unwelcoming, or even inaccessible, for citizens from more diverse backgrounds than the more homogeneous members of WNCP groups. The potential normalisation of discriminatory behaviour and acquiescence by the police to these practices make it difficult to determine who is responsible for an open neighbourhood environment and who can be held accountable when tensions and conflicts arise from discriminatory WNCP group practices.

App: Inform the WNCP network via WhatsApp

When the intended SAAR process is followed, this is the stage where WNCP members are supposed to inform the WNCP network about the suspicious situation they have encountered and already reported to the police. Ideally, this is also the point at which the group member can forward police instructions to the WNCP members in order to direct citizen actions. However, as noted above, this phase often occurs before or even in place of notifying the police. Regardless of whether the police are included in the process or not, this moment is the crucial component for the existence of WNCP groups themselves – this is the time in which (vital) security information is passed on to other neighbours.

Ideally, all neighbours that live in a particular area would be involved in the WhatsApp group in order to ensure the widest range of coverage and increase the likelihood of a secure and safe neighbourhood. As such, most moderators make substantial efforts to include as many neighbours as possible in their groups, however, not all community members are part of the WNCP groups. Participation levels vary across neighbourhoods. For instance, group moderator Louise estimates fairly high participation in her neighbourhood: “*I believe we have 100 houses in the street, and 70% is part of the group*”. In Bert’s village, with a population of 1200, his group covering the whole village only has 167 members.

Moderator Marc even describes a difference in participation rates between his two WNCP groups. One neighbourhood is larger and includes citizens of many cultural backgrounds, but that WNCP group has considerably less members than the group in the other neighbourhood where the population is more homogeneous. When asked about a reason behind this difference, Marc stated: *"I think that it is, eh, socio-culturally determined...People might not know about this or maybe even feel less responsible for their neighbourhood".* Although his comment that people in culturally diverse neighbourhoods may take less responsibility is unfounded, it illustrates that it can be difficult for moderators to connect with particular groups that may diverge from their own personal cultural or ethnic heritage. This comment also shows a fairly common fact amongst the WNCP groups in our sample: they are more popular among homogeneous Dutch groups. Even with efforts to reach out to culturally diverse members of such groups, the interview and focus group respondents predominantly had a Dutch background (mostly white, Dutch-speaking and of Dutch cultural origin). The lack of diversity in WNCP groups seems to reinforce the uneven and discriminatory power relations mentioned above in neighbourhoods with more diverse populations. Arguably, the lack of diversity within WNCP groups may perpetuate problematic discriminatory practices.

The issue this raises is that in participatory policing campaigns, not everyone can freely participate. Rather, based on specific traits or behaviour, some persons can be seen primarily as potential threats instead of actors that can participate in policing activities. *"Only a privileged few get to be watchers, i.e. those who comply with authority, agree to play the reporting-game, and 'fit in' as usual and ordinary elements of society"* (Larsson, 2017, p. 98). This is evident in WNCP groups; while seemingly open to all interested neighbours and not only a privileged few, citizens do have to abide by the rules of the group and fit in with the WNCP practices and mentality in order to successfully participate. If members break the rules, moderators have the power to remove them from the group. WNCP group moderator Louise describes her responsibilities: *"My duty is about the importance, a bit of awareness, and to try to prevent calamities, to prevent discordance, or that things are followed up incorrectly (…) It is sometimes a bit of a mediator role, ha-ha"* (Louise, WNCP group moderator).

Group moderators make themselves responsible for gate keeping and controlling the groups, though often they share these responsibilities with one or more other moderators. Here is where the power dynamics differ between participatory policing campaigns and WNCP groups, as the rules and actions are policed by citizen moderators instead of government actors. Additionally, WNCP group conversations are largely transparent to the members themselves, because they may see incidents unfold in the group and receive a message when group members are either removed or remove themselves. Yet these processes related to group moderation can be seen to perpetuate an uneven power balance between the moderators and the members, leading to frictions within the group. Moreover, there is also an uneven power balance between WNCP group members and other neighbourhood residents based on visibility. For non-members it is unclear how many of their neighbours are part of the groups and how these neighbours might also be seen to keep an eye on them. Even though group moderator Rob assures that the group will also help non-members: *"When these people need help, of course, we will never hesitate to jump in and help them out",* non-members lack direct access to other people in the neighbourhood. Group conversations that take place on the smartphones of WNCP members and remain invisible to other neighbours. Non-members may be unaware of citizen-initiated events unfolding in their streets and do not know if and when they are the subject of WNCP suspicions or actions.

Again, the make-up of WNCP groups is diverse. In a number of WNCP networks, police actors are actively or less actively involved. Appendix 1 indicates that in several groups police are not involved at all. In relation to his group, moderator Kai says: *"The police do not want to be involved, we think that that is a pity".* When asked for an explanation about why this may be more generally, community police respondents in our research unanimously said that they fear an overload of messages: *"If I would join the group, I am sure I would be responding to messages day and night"* (Jim, community police officer) Some community police officers avoid this by not joining the WhatsApp group with all the members; rather, they are connected only to the moderators in a separate WhatsApp group. Yet, there are also community police officers who deliberately choose to be part of the neighbourhood WhatsApp group. In this way, some group moderators feel they can benefit by having a direct line to the police department in the group: *"We have a community police officer in the group... He has a police radio and can directly call the control centre to ask why a notification is not followed up"* (Dave, group moderator). In addition, neighbours can ask their community police officer directly for advice when they are not sure if they need to call the public alarm number for an incident: *"Often, we first consult our community police officer"* (Arnold, group moderator). Arguably, the involvement of community police officers can lead to shared responsibilities and accountability with regard to neighbourhood safety, crime prevention and a sense of community.

However, as suggested, the (in)direct involvement of police also has downsides. Group moderator Bert explained that his community police officer is actively involved: *"So he also reads everything".* Of course, when police officers read the content of WNCP groups, they are simultaneously monitoring citizens in the groups. This form of monitoring can be somewhat invisible, particularly because group members are often unaware of the presence of a police officer in the group. These groups only include a list of phone numbers which, with the exception of moderators who are listed as *beheerder* in Dutch or admin in English, do not automatically indicate members' names or roles. This subtle monitoring may enable a community police officer to know certain things about the neighbourhood or even when and how to mobilise which neighbour:

> *"Well, I have people in the street who have webcams placed in their windows, and when you make an inventory of the WNCP group members, like, he has a dog, that person works at night, she comes home at two AM and walks the dog ...You can use that directly."* (Rick, community police officer)

But the invisible monitoring of citizens can become problematic when WNCP group members fail to abide to the rules or share details about how they actively engage in *citizen policing* in ways that might not be legal. Even though the conversations within WNCP groups are transparent, the (police) actors involved often remain invisible to most members. Community police officer Ron explains: *"They don't want the community police officer looking over their shoulder".* As such, there is limited clarity about the involvement of police within these groups and their connection with moderators or other groups, something that needs to be worked out more completely. Despite being a *citizen* based movement open to all to participate at a local level, the homogeneous nature of many groups, the fact that they are only open to citizens following the WNCP mentality, and the often-invisible involvement of police actors show that they are not that free, open, or transparent.

Reageren: React in a safe manner

Despite the complexities noted above, in the idealised situation, once suspicious activities are identified, the police are alerted and WNCP actors are informed, the final stage of the SAAR method is reached. The intention for this phase of response is to disrupt the activities of those seen as suspicious by actively intervening. The guidelines emphasise that this should only be done safely, avoiding risks, for example by approaching the suspicious person with some small talk ('Huisregels', 2015). Moreover, showing that you are watching can also be seen as a way of intervening: *"Reacting, well, that's also, just pulling aside the curtain to watch what's happening"* (Ron, WNCP group moderator). This last step in the SAAR process suggests that these participatory policing practices can lead to the prevention of crime or apprehending criminals. Group moderator Louise describes how citizens and police collaborated in the arrest of two burglars:

> *"Two guys were arrested in the street...They fled from another street and were walking through our street. Then the police were called and informed via the neighbourhood app: 'they are now at number something, and they are walking in that direction'...The police, who were already informed, were able to throw them to the ground. So that was a good action."* (Louise, group moderator)

While this more or less fits within expectations of the SAAR process, WNCP members often first inform their network before they alert the police. Sometimes this can lead to activities or behaviour that go against police desires or instructions. Emma describes:

> *"We've had a situation with a dark-skinned man at the [name of street] who was reported, and everyone went out to look for him. Even though someone reported: 'the police are informed', they started searching for him anyway."* (Emma, group member)

This incident depicts a moment in which WNCP group members attempt to actively safeguard their neighbourhood – they take this responsibility onto themselves rather than wait for the police to deal with the situation. In some cases, the WNCP activities may jeopardise police investigations. Group moderator Dave describes a situation where WNCP members interfered with a police case:

> *“Some time ago, we had an incident with a drug dealer and 4-5 people alerted the police and were wondering if something was happening. But it turned out that they already had the group in view but didn’t want to intervene because they wanted to know what else they were up to.”* (Dave, group moderator)

In another group, citizens interfered with a police drill about a fake burglary and an escape by car: *“And before the car was there, it did not go as planned, because a group of men was waiting for the car with baseball bats. So, they had to cancel the drill”* (Ron, group moderator). It seems that though WNCP groups actively request police visibility, they may also create significant tension due to the invisible nature of many police practices.

Even beyond this, in some groups, neighbours bypass police completely and start their own investigations and actions. Betty, group moderator in a village, often collaborates with another active WNCP group member: *“I saw a potential burglar in the afternoon, and I followed him...Later we reported this to the police, and Theo [group member] found the same person on his camera footage. So, we reconstructed that [incident]”* (Betty, group moderator). So, even when WNCP networks include police members as in this case, citizen safeguarding activities might remain unnoticed by the police, despite the fact that in this process they can harm themselves or intentionally or unintentionally harm the allegedly suspicious people they follow or approach.

When citizens assist police in actively monitoring the street or by interfering with criminal activities, the boundary between police and citizen territory becomes fuzzy. According to Bas, community police officer, this boundary even disappears:

> *"When citizens report a suspicious situation, they are actually doing police work. So, eh, there is no boundary …We would like citizens to facilitate us in the arrest [of an offender] by telling us where he is, but, honestly, we prefer that citizens don't make arrests themselves."* (Bas, community police officer)

This represents a key comment illustrating the blurring of boundaries between police and citizens (Reeves 2012). When citizens actively monitor their streets, record events, and report about suspicious situations or persons, they are informally taking over police duties. Citizen policing (a term which is interestingly not directly translatable to Dutch, see Pridmore et al., 2018) raises questions about accountability and responsibility. Mobilised citizens may act as *"embodied surveillance units"* (Larsen & Piché, 2010, p. 98) who become responsible for the security of themselves and others, but can they also be held accountable when their safeguarding practices fail or a dangerous situation escalates? The citizens in WNCP networks often operate on the basis of intuition and instinct, lack professional training, and can further be motivated by excitement. *"I have to be honest, I always find it very exciting and am really curious...If I know it's near my house, I'll think: Let's take a look"* (Jessica, group member). The motivations of WNCP group members (often) remain invisible though this can have an enormous impact on the safety of themselves and others in the neighbourhood. In this way, the responsibilisation of citizens may lead to certain forms of risky vigilant behaviour that can then create even riskier situations that arguably the formation of these WNCP groups were intended to reduce (Larsen and Piché 2010).

Conclusion: Minimising obtrusive surveillance practices

By examining each of the steps in the promoted SAAR method for WNCP groups, our analysis highlights a number of issues. Most importantly, we focus on the responsibilisation of citizens to participate in and take care of their own neighbourhood. As this happens alongside the members' desires to engage in promoting security, the everyday activities in these groups often default to more problematic forms of lateral surveillance. As noted above, this includes an increasing distinction between *insiders* and *outsiders,* the normalisation of suspicion, a potential reinforcement of discriminatory practices, challenging relations with the police, and the potential for illegitimate citizen actions. All of this is occurring in a *free* forum that has a number of both formal and informal expectations placed upon its members.

Yet the focus here on these problematic issues should not outweigh the growing popularity of these groups – many Dutch citizens have become willing partners in citizen-led crime prevention groups. Participation in these groups varies; interpersonal connections with neighbours in these groups varies; discrimination against outsiders varies; and relations with the police varies, etc. Yet, it is hard to overlook something which might be seen as one of the most successful forms of participatory policing occurring at a local level, at least in terms of its rapid growth. Given our highly critical accounting of this practice, what then can be made of this phenomenon? How can we minimise the more obtrusive surveillance practices and allow for the potential social benefits that have perhaps made these groups so popular? To that end, we present three important suggestions.

First, what is clear is that **increased transparency is needed in how these groups interact with more formal police structures.** This is something that needs to be addressed in this particular case by the police in The Netherlands, and potentially in Germany and Belgium where WNCP groups are also gaining popularity. Other engagements with citizen-led participatory policing or social media style information groups that have *security* related components (such as Nextdoor) will likewise require an increasingly clear delineation about how police will and should participate with these groups. But in our specific case, moderators of these groups also require some systematic or regular informational messages being sent about the group purpose and the groups connection with the police to increase transparency. As far as we have determined, this only happens on a limited and ad hoc basis.

This raises our second suggestion, that although the SAAR method has its value, the method is also **limited in addressing the ambiguities of neighbourhood crime prevention situations.** Although these groups are built on a low threshold for access and participation, an increased flow of information is needed regarding the most appropriate use of these groups. Strategic and informational campaigns may help reduce some of the more discriminatory practices our research has uncovered, but this also may begin a more public dialogue about what local involvement and engaged citizenship may look like in a digitally connected era. We further see that this engagement should be built on our third suggestion, initiatives should be made to **develop purposeful trust building amongst neighbours and within neighbourhoods,** particularly where there is a diverse population. This may be the most challenging suggestion given the seeming reinforcement of dominant cultural narratives and expectations in these particular groups, but these are efforts that can increase the potentials for (democratic?) unity and a more representative citizen involvement.

Limitations and suggestions for future research

Given our evaluation of these WNCP groups and their implications for increased surveillance, these suggestions are perhaps a bit obvious. However, they actually require further substantiation. We note that our research is limited to largely homogenous groups which demonstrated some discriminatory practices. Experiences of those from more diverse backgrounds that both are involved in and purposely choose not to participate would greatly increase our understanding of these groups. Further, this research would benefit from a more systematic understanding from the policing side in terms of policy developments related to citizen involvement in policing (as recommended in Lub & De Leeuw, 2017).

Although there remain clear implications on the policy domain, we have not detailed this here given our primary focus on citizen practices. We have likewise focused only on these messaging applications, whereas Dutch citizens learn about police activities and respond and engage with their actions in a variety of formats including numerous social media channels, websites, and forums. How these media intersect with these messaging groups would provide a richer understanding of the digital means for participatory policing practices.

While a WNCP street sign may act as a visual marker of a mainly invisible crime prevention network, the actual practices of these groups remain largely invisible to outsiders. This has created and may continue to create precarious situations in many Dutch neighbourhoods which are in part related to the blurring of boundaries between citizens and police (see Reeves, 2012). As citizen initiatives, WNCP networks are themselves the impetus leading to the responsibilisation of citizens, something of which, to varying degrees, police have made use. But this responsibilisation further generates issues of accountability within these formal and informal modes of policing, even when a SAAR type approach is employed. The context of these specific practices may be unique to The Netherlands, yet the more general drivers of surveillance in this case – the protection of homes, the appeal of looking, increased social connections, the feeling of doing something good, succumbing to curiosity amongst others – are more universal. When we examine participatory policing practices more generally, it is the interrelationship between these drivers and their social (and political and economic) effects that require careful consideration – something this chapter has only begun to detail.

PART 2

Boundary sculpting practices in communicative contexts

Chapter 5

"Nobody needs to see when I'm online" Everyday boundary work practices[6]

Introduction

Saskia lives in a quiet neighbourhood in a mid size city in the Netherlands. She works at a primary school, has two children, practices yoga, has an active social life, and participates in a neighbourhood crime prevention group. She uses WhatsApp to keep in touch with her family, friends, fellow yoga practitioners, neighbours, colleagues, and many others. For her, WhatsApp is convenient, especially because its functionalities allow her to monitor if her messages have been received and read. At the same time, Saskia also struggles to keep track of all the different conversations. When she receives neighbourhood messages at work or messages from colleagues during the weekend, the boundaries between different contexts become blurry. Saskia often experiences pressure to respond and feels WhatsApp conversations can invade her privacy.

Saskia is one of our interview respondents and she is not the only one who experiences messaging apps this way. The ability to communicate with colleagues, neighbours, family, and friends across the world has never been easier. Mobile devices and messaging apps such as WhatsApp, iMessage, and Signal collapse temporal and spatial distances and create potential for constant networked connections (Burchell, 2015). While they enable people to engage in asynchronous mobile conversations not bound by place or time, messaging apps can also be perceived as volatile, addictive, immediate, distractive, and privacy invasive (Mascheroni & Vincent, 2016; Park & Mo Jang, 2014; Pielot et al., 2014; Storch & Ortiz Juarez-Paz, 2019; Sultan, 2014). In order to cope with the communication overload caused by continuous interactions (Licoppe, 2004),

[6] This chapter is a slightly altered version of: Mols, A., & Pridmore, J. (2020). Always available via WhatsApp: Mapping everyday boundary work practices and privacy negotiations. *Mobile Media & Communication, 9*(3), 422-440.

individuals actively manage boundaries between different relational contexts, and between being absent and present.

To understand and contextualise these strategies and practices, we explore the ongoing management of boundaries as forms of boundary work (Clark, 2000; Nippert-Eng, 1996a, 1996b). Our research focuses on messaging practices in the Netherlands in order to answer the research question: **How do individuals use functionalities of messaging apps to sculpt boundaries in asynchronous communication across different relational contexts?** The example of Saskia demonstrates that everyday use of messaging apps blurs the boundaries between family life, work contexts, community activities, and social contacts. While most existing studies focus solely on the blurring boundaries between work and private life (Jahn et al., 2016; Olson-Buchanan & Boswell, 2006; Schalow et al., 2013; Vitak et al., 2012; Walden, 2016), this chapter expands beyond the professional/personal binary in order to consider boundary work in more nuanced relational contexts including children, partners, friends, neighbours, and colleagues.

We aim to provide a better understanding of the complexities of boundary work practices by presenting an in-depth account of the use of WhatsApp by two different groups of respondents. The first group consists of employees in a variety of Dutch workplaces, ranging from multinational companies to restaurants. The second group contains moderators and participants of WhatsApp Neighbourhood Crime Prevention (WNCP) groups, a popular phenomenon in the Netherlands. In these WhatsApp group conversations, neighbours exchange warnings, concerns, and information about suspicious activities in their neighbourhood (Lub & De Leeuw, 2017). We explore how respondents from these two groups of WhatsApp users engage in boundary work in order to manage constant networked connections.

The next section explores literature about the benefits and pitfalls of constant networked connections, the collapsed dichotomy between absence and presence, and boundary work strategies. The results section adds to this body of research by providing an overview of messaging strategies our respondents use to manage their privacy, freedom and autonomy in relational contexts surrounding work and neighbourhood connections. Our research highlights two different forms of boundary management. On the one hand, respondents safeguard their personal time by deliberately being absent from digital interactions. On the other hand, they actively sculpt boundaries between different contexts.

Literature: Connectivitiy and boundary management

This section provides insights into the consequences of the constant networked connections that go hand in hand with smartphone use. On a daily basis, people have to cope with information collapse and information overload which requires them to manage the boundaries between absence and presence constantly. And although Nippert-Eng’s (1996a, 1996b) seminal work on boundary theory precedes smartphone use as we know it, she provides key concepts that help understand how people sculpt boundaries between professional and personal contexts.

Constant networked connections and context collapse

Smartphones are integrated in everyday routines and individuals have an ambivalent relationship with this domesticated technology (De Reuver et al., 2016). Smartphones enable long distance connections and can offer assurance and feelings of safety. However, they can also cause social disconnection when distraction and misunderstanding lead to negative emotional responses (Storch & Ortiz Juarez-Paz, 2019). Smartphones enable asynchronous and continuous interactions via messaging apps. Messaging apps embody what Burchell describes as *“the contemporary communication context of constant networked connection”* (Burchell, 2015, p. 40). Networked communication practices take up time, attention, and energy of individuals, who continuously need to devote attention to their devices, platforms, and applications. Messaging app interactions are asynchronous and seem devoid of temporal boundaries. Yet messaging apps require real, situated, and time-consuming activities by individuals (Burchell, 2015).

The use of messaging apps can create intimacy, proximity, and security while it can also lead to anxiety, exclusion, obligation, and communication overload (Mascheroni & Vincent, 2016; Stephens et al., 2017). Using multiple communication channels and devices overwhelms individuals with information and piled up messages, while distracting them from the current situation. Mobile devices and messaging apps embody the expectations of others because they create responsibility and pressure to respond (Stephens et al., 2017). In contrast, networked practices can also reduce stress because they enable individuals to create flexible social arrangements and allow them to shift activities and interactions (Bittman et al., 2009). Futhermore, smartphones constantly trigger the user’s attention via notifications such as alarms, blinking lights, alerts, and ringtones. These are often perceived as valuable, yet, they are disruptive by nature and can cause stress (Licoppe, 2010; Shirazi et al., 2014).

Moreover, within messaging apps, all conversations are located in the same digital space and there seem to be no tangible boundaries between different contexts. Conversations with family members are part of the same digital collection of messaging flows as group conversations with colleagues, and interactions with neighbours, friends, and other contacts. Messaging apps default to context collapse because the boundaries between different types of contacts are automatically flattened into one singular group (Vitak et al., 2012). Notably, context collapse goes beyond online contexts because technologies also collapse offline contexts when the Internet is incorporated in daily practices (Pagh, 2020).

Managing boundaries in constant networked connections

The use of WhatsApp and other messaging apps collapses the boundaries between contacts in different contexts, as well as temporal and spatial boundaries between these contexts. Our research identifies and explores two forms of boundary management practices. The first focuses on creating boundaries between absence and presence. The second highlights practices to manage boundaries between different communicative contexts. These two forms of boundary management are further contextualised in the next sections.

Creating boundaries between absence and presence

The ability to have mediated interactions leads to connected relationships in which the boundaries between presence and absence become blurred (Licoppe, 2004). People are simultaneously absent and present in the lives of others when they are in continuous contact via messaging apps. Many people use multiple communication channels on their smartphone, such as messaging apps, social media, work email, and dating apps. Disconnecting can be a way to escape from digital interactions and the expectations these create. Mannell (2019) describes *disconnective affordances* which can be used to reduce distraction. These are opportunities to disconnect facilitated by the materiality and features of mobile platforms and devices. The most far-reaching affordance is *signal jamming*, which creates unavailability on all channels by switching the phone off or by enabling airplane mode.

However, more often strategies to cope with the pressure of digital interactions are less absolute and take place against a backdrop of constant connection. Burchell (2017) describes how individuals actively construct unavailability on specific channels when they engage in purposeful practices of being absent. Individuals negotiate networked absence, a deliberate lack of engagement within networked connections. A distinction is created between being aware of interactions and engaging with interactions, and actively making this distinction provides control over the flow and organisation of communication (Burchell, 2017). Purposeful practices of networked absence are exemplified by the other disconnective affordances that Mannell (2019) presents. The affordance *disentanglement* refers to loosening the ties between device, platform, and person by switching off particular notifications, or by placing the phone out of sight. Individuals can also *modulate* availability by blocking particular contacts or leaving group conversations. Via *delay* individuals postpone their responses, and finally, with *suggestiveness* minimal and curt messages are used to discourage extensive and detailed conversations (Mannell, 2019). This chapter builds on Mannell and Burchell’s observations by considering how different relational contexts and specific features of messaging apps shape the way people sculpt boundaries between absence and presence.

Sculpting permeable boundaries between different contexts

Due to the default collapsing of contexts within messaging apps, individuals are continuously available to different relational contexts. As the introductory chapter indicates, boundary theory provides helpful tools to understand how people construct, maintain, and modify boundaries between different contexts in their lives (for an overview of boundary theory see Jahn et al., 2016). According to Nippert-Eng (1996a, 1996b), boundaries can be seen as sociocognitive borders between cultural categories. These borders are permeable, which means that elements from one domain can enter other domains (Clark, 2000). People actively work to reproduce and challenge boundaries on a continuum from *integration* to *segmentation*—from no distinction between two contexts (e.g., work and private life) to a rigid separation of different segmented worlds (Nippert-Eng, 1996b). Objects, activities, and tasks reinforce the different territories put in place, for example, the use of keys differs across employees: people who separate work from private life can have two sets of keys, while people who integrate the two contexts might have a large and mixed set of keys (Nippert-Eng, 1996a).

Boundaries are not rigid, but can be flexible depending on the demands from the domains which they separate (e.g., flexible work times determine particular temporal boundaries) (Clark, 2000). The use of technologies increases the permeability of borders between work and private life, because technologies such as smartphones can physically bring work into private domains (Olson-Buchanan & Boswell, 2006; Sayah, 2013). Notably, the use of social media also introduces personal content and personal communication into the workplace (Siegert & Löwstedt, 2019). High levels of flexibility and permeability can lead to a *blending* of contexts. In order to deal with this blending of work and home contexts, people devise strategies. They can decide to disconnect work technologies or to ignore them during weekends or holidays (Duxbury et al., 2014; Siegert & Löwstedt, 2019). Others set aside time to address workplace communication (Burchell, 2015), e.g, after their children go to bed (Duxbury et al., 2014). People also devise tactics around personal communication during their work day, such as checking social communication channels but postponing responses until after work (Burchell, 2017). Whereas these studies show the diversity of boundary work strategies for work and personal life, boundary sculpting practices become even more intricate when other contexts are also involved. Therefore, our research is based on interviews about everyday boundary work practices of Dutch WhatsApp users across different relational contexts.

Research method: Interviews and focus groups

Boundary work is part of everyday actions. In order to make sense of everyday activities, our qualitative research design explores messaging practices. This approach inspired by existing research focusing on practices, such as smartphone practices in schools (Merchant, 2012), Facebook user practices ((Van House, 2015), and interactions between individuals and the Internet (Carstensen, 2015). Methodological details about the practice theory approach, sampling, and constructivist grounded theory analysis (Charmaz, 2014; Corbin & Strauss, 1990) can be found in Chapter 2 and the resulting codebook is included in Appendix 12.

In order to include multiple contexts, this chapter is based on two data sets – the WNCP sample (Appendix 1) and the work messaging sample (Appendix 2), resulting in a corpus of 43 interviews. Messaging practices were included in the two interview guides for these two sets of respondents (see Appendices 5 and 6). Specifically, the two topic lists overlapped in sections about everyday messaging practices, availability, notifications, the use of specific settings, reaction speed, and the use in different contexts. Due to WhatsApp’s functionalities being similar to other messaging apps, our results about WhatsApp can be seen as exemplifying messaging practices in general.

Results: Managing absence and segmenting contexts

When using messaging apps, individuals often deploy strategies to manage availability. On the one hand, they manage boundaries between being simultaneously present and absent. On the other hand, they devise tactics to integrate or separate messaging flows from different contexts. In this results section, we highlight how these two forms of boundary management revolve around digital and material functionalities of smartphones and WhatsApp, and how they are integrated into everyday relational contexts.

Demarcating absence and presence

The most straightforward way to create absence by disconnecting is *signal jamming* by switching off the phone (Mannell, 2019). However, as Burchell (2017) describes, managing absence and presence is often less absolute than fully disconnecting. And indeed, most respondents told us that they never switch off their phone, yet, they use specific settings to deal with the pressure caused by being always available.

Activating silent mode for temporary absence

For many respondents, activating silent mode forms a strategy to avoid the pressure and distraction caused by notifications (Licoppe, 2010; Shirazi et al., 2014). For instance, Kenneth (manager in a zoo) uses silent mode to limit distractions during his workday: *"Often my phone is in my pocket and eh, it doesn't buzz, so I don't get a signal that I received an app [message]. Otherwise, I'd go crazy".* Similarly, WNCP moderator Ron wants to be informed but he does not want to be interrupted by notifications: *"My phone's never off, it is always on. But I don't hear or see everything. Yet, it's always on, often on silent mode ... I like to know what's happening".* Kenneth and Ron want to remain present for all their contacts when they are physically absent (Licoppe, 2004), but prefer not to be constantly distracted.

Notably, strategies to create temporary absence are motivated by the meaning attached to different communication channels and contexts. WhatsApp provides an additional communication channel in work contexts, whereas it forms the main (and in most cases only) means of interaction in WNCP groups. The smartphone is the only tangible object of a WNCP group, so being unavailable means not being part of safeguarding practices, and potentially *failing* to meet neighbourhood expectations. Being available and informed has thus another meaning and other consequences in neighbourhoods than in work contexts. WNCP moderator Bert does not mind the distractions because he feels he needs to be up to date about what happens in his neighbourhood. Though, there are limitations to his availability: *"When you have your phone on, a WhatsApp message will come in, beep beep. Well, that's fun in the middle of the night. You'll be wide awake, thinking: What's happening!?"* In order to prevent this from happening, Bert activates silent mode during the night.

Being visibly present: The last seen setting

WhatsApp (as well as other messaging apps) includes a particular feature to check when people have been active on the application. For each conversation, this setting is by default indicating *"last seen on..."* with the last time the contact was online. This feature amplifies the notion of presence and absence on WhatsApp because it allows individuals to form expectations based on the last moment a respondent was active. If this is just a few minutes ago, being absent might be conceived as less absent than when the respondent has not been active since two days. This feature has been seen to lead to strong expectations and social pressure (Pielot et al., 2014), but it can also form an indicative object of individuals' boundary management. The last seen setting can only be disabled for all contacts at once, and works reciprocally—users who choose to disable this feature are unable to see the last seen setting of others. Thus, WhatsApp allows individuals to use the last seen setting as a purposeful practice of being absent (Burchell, 2017), yet they are constrained by the reciprocal nature of the setting.

For some, the last seen setting is a useful feature. In one of the focus groups about WNCP messaging, Emma mentioned that she checks how late her WhatsApp contacts were last seen online: *"I check if he or she is still awake". In response, Bianca, another participant, stated to Daniel: "You switched it off!"* Upon which Daniel replied: *"Nobody needs to see when I'm online. If they need me, they can call me. And if I don't answer, I don't answer".* Emma's practices show that she has a clear purpose, combined with knowledge about WhatsApp affordances. In contrast, Daniel's attitude shows that he is not hesitant to use the delay tactic; he answers when he wants to (Mannell, 2019). He disables the last seen setting for the purpose of maintaining boundaries between absence and presence. Clearly, there are different orientations towards what contacts can and should see.

Marian (WNCP group moderator) disabled the last seen setting in order to maintain the boundaries between her personal life, neighbours, family, and friends: *"Sometimes, I am awake in the middle of the night, and then someone will tell me: 'Jeez, were you online at 2:45?' I really do not want everyone to know".* For Marian, the last seen setting served no purpose and its use had a negative meaning because it invaded her carefully segmented life. She felt the last seen feature invaded her privacy by displaying information about her WhatsApp use to all her contacts. To disable this feature, she needed specific knowledge about WhatsApp's settings and how to change them. Moreover, she first needed to develop the self-awareness that the setting was bothering her before she could disable it. She then used it to thicken the boundaries between herself and her WhatsApp contacts. For Erik (account manager), the last seen setting has a different connotation. He values his time off and does not want to feel work pressure outside of work hours. Erik therefore disabled this feature *"because it can create expectations…that someone says: 'I can see that he's been online, but he didn't do anything with my message yet'".* Disabling the last seen setting enables Erik to keep his work life integrated in his personal life while minimising the pressure this integration can bring.

Response accountability: Blue checks

The *blue checks* feature of WhatsApp provokes similar responses. When a message is sent, one gray check symbol is visible—once this message is delivered, a second check appears; and finally, when the receiver opens the message on his device, the gray checks turn blue. These blue checks are an indication to the sender that his/her message has been read. Again, WhatsApp amplifies the experience of presence and absence in interactions, because when the blue checks appear, the purposeful practice of being absent becomes visible to the respondent. Without the blue checks, individuals can make a distinction between being aware of interactions and actively engaging in interactions (Burchell, 2017, p. 20). The blue checks form the material embodiment of this decision process because the sender can directly see when the respondent is aware of the message, but has chosen not to actively engage in the conversation, at least not yet. Notably, this feature can only be disabled for one-to-one interactions and not for group conversations.

This can be particularly precarious in WNCP conversations when expectations might be based on the fact if a person read a message (e.g., when a neighbour asks for help and others read the message but do not respond). In one of the focus groups, it became clear that this feature also allows the sender to see which participants read their message at what time. WNCP moderator Betty explains: *"When I post a message in the app [group conversation], when I do this [swipes over her phone], I can see who read my message. I discovered this! Look [shows WhatsApp conversation on her phone], 17 past 10, 27 past 10…You, Vera, you read it at 13:50 and your husband even a day later".* The other respondents react surprised; they did not know about this feature.

The fact that some respondents are not aware of this possibility displays a divide in technical knowledge among participants of WhatsApp group conversations. Moreover, for unaware participants this feature creates a potential privacy invasion that remains invisible until action is taken as a response to the blue checks. Overall, our interviews revealed different attitudes towards the blue checks. Whereas many respondents actively use it, Victor disabled the blue checks feature:

> *"Because I find it really annoying, and I've experienced this, that people message me: 'Why don't you react on WhatsApp, you opened my message at that particular time'? So that constraints my freedom. I do not feel like justifying why I didn't react. Why should I justify myself that I do not immediately respond to someone who enters my privacy, eh, private sphere?"* (Victor, government official)

While Victor explicitly creates boundaries by disabling the blue checks to protect his privacy, Lenny (WNCP group moderator) feels less able to follow Victor's strategy. His boundary management practices are the result of social considerations:

> *"For me, blue checks are visible because my wife makes me, ha-ha. I switched them off [the blue checks], but eh she cannot handle that, ha-ha. She said: 'I want to know when you're online, why did you switch off the blue checks?'"* (Lenny, WNCP moderator)

Lenny and his wife both attach a different meaning to WhatsApp's blue checks. Whereas Lenny likes to maintain boundaries between different relational contexts and wants to disable the blue checks, his wife wants to be able to tap into her family context while she is apart from him. This disagreement leads towards a forced blending of boundaries (Clark, 2000), providing an example of how online contexts are integrated into offline contexts (Pagh, 2020). The collapsing of Lenny's personal offline context with his personal online context became tangible when he discussed the blue checks with his wife.

Lara (graphic designer) uses the blue checks feature to monitor the responses of her contacts. However, at times, she does not want her contacts to know that she read their messages, and for those instances she devised a tactic: *“But there’s a trick, you know? If you put your phone on airplane mode, you can just open WhatsApp and read all your messages and they will not get blue checks”.* Lara makes a deliberate distinction between contacts she wants to be able to see that she read their message, such as her mother and her best friends, and other contacts that she wants to hold off on, such as colleagues. Such granular boundary sculpting practices require technical knowledge. Lara’s advanced knowledge about the functioning of WhatsApp and her smartphone influences her messaging practices. Greater levels of technical savviness lead to more advanced boundary work practices. (A lack of) knowledge is known to influence human–computer interactions (Carstensen, 2015), and proves to also influence messaging app interactions and related boundary management practices.

Segmenting smartphone contexts and sculpting boundaries

The second form of boundary management described by our respondents regards the active sculpting of boundaries between different contexts. In view of Nippert-Eng’s work (1996b), practices range from rigid segmentations to integrated contexts. Respondents use smartphone affordances and WhatsApp functions to manage the presence bleed (Walden, 2016) from WhatsApp conversations into different contexts.

Do not disturb mode for context segmentation

A smartphone brings elements of other contexts into the current context and enforces permeable boundaries (Clark, 2000) and context collapse (Pagh, 2020). Most smartphones include a *do not disturb* mode which can be activated to block phone calls and notifications. This mode can be used as a disentanglement strategy in order to disconnect temporarily from most contacts (Mannell, 2019). Many respondents put up temporal boundaries to protect themselves from distraction and pressure, and to be fully present in one context and absent in all others. Most of them use the do not disturb mode to protect their private context. For example, Erik (account manager and volunteer scout leader) wants to spend his personal time without interference from other contexts such as his work or scouts' group: *"After 9PM, I do not feel the need to, eh, to immediately, that thing [smartphone], when something comes in, to respond immediately".* The do not disturb mode functions as a digital lock on his availability. The use of this mode is motivated by the purpose of protecting private time, and requires knowledge about smartphone affordances.

Key to the do not disturb setting is that individuals can make exceptions for contacts that can ring through. This form of modulation (Mannell, 2019) allows users to create segmentations in their social contexts. For instance, Jennifer created a distinction between contacts that she blocks and specific contacts that can reach her any time:

> *"At night, I always put it [smartphone] on do not disturb, but the sound is on, and it rings when my favorite contacts call me. My best friend and my parents are in that group, because I have the feeling that when they call me during the night, it is about something important. And then I want to be there for them."* (Jennifer, server in restaurant)

Similarly, Lea (manager in a hotel) also created a list of people who can reach her when she activated the do not disturb setting: *"My children, the father of my children, my father, my sister, my partner, my best friends. That's it. A short list".* Jennifer and Lea sculpt a boundary between contacts that have to be able to reach them at all times and contacts that they prefer to be unavailable to. This segmentation enables them to tune out of conversations with most contacts but to remain available for a selection of important people from their closest social context.

Prioritising contexts while managing communication overload

Many respondents experience stress because of the large amounts of messages from different contexts they have to process on a daily basis. They have to deal with communication overload (Stephens et al., 2017). For instance, Ciara (consultant for start-ups) is ambivalent about the use of WhatsApp: *"It's the worst and the best thing at the same time". In* *general, she likes WhatsApp, but when she receives messages from her work context late at night it becomes a stress-factor: “So that is really this double edging, in a way, it is overloading”.* Respondents express concerns about excessive amounts of messages that they receive from their family, colleagues, friends, neighbours, and other contacts. They actively sculpt boundaries between more and less important contexts by using WhatsApp settings to manage all their conversations, and to create material distinctions between contacts from different contexts.

Unread and archiving to organise messaging overload

In order to cope with communication overload, respondents devised several strategies. Mark (municipal official) tries to maintain a grasp on all his conversations by marking important conversations as *unread*: *“So that I know: ‘Oh, yes, I need to do something with that message”.* Another strategy was explained by Erik (account manager), for whom a WhatsApp inbox full of conversations creates unrest. In order to shut off particular contexts, Erik archives all complete or inactive conversations. WhatsApp enables users to move conversations to the archive which makes them invisible. Conversations become visible again as soon as a new message is sent or received (or if they are manually moved back to the inbox). Practices such as archiving and marking messages as unread enable individuals to manage messages in a way that fits their needs and to prioritise conversations from particular contexts. This is a clear example of how WhatsApp provides specific means to enable users to exercise control over if, how, and when they address particular interactions (a strategy also described by Burchell, 2017). WhatsApp app not only enables users to create order in messages from different contexts, but also to create material distinctions by muting conversations or by changing notification sounds.

Different sounds for different contexts

By default, there is no distinction between different types of WhatsApp conversations. However, individuals can use particular settings to create tangible distinctions between different contexts. These boundary management strategies require detailed knowledge about WhatsApp functionalities. When it comes to neighbourhood safety, WNCP group messages are perceived as more urgent than other conversations. A WNCP message can, e.g., warn neighbours about a house break-in, in which case immediate action is desirable. In order to distinguish a message from a particular context from other conversations, people can install distinctive notification sounds. To illustrate, Saskia (WNCP group moderator) uses a different sound for WhatsApp messages in the WNCP group: *“So I can check directly”.* Similarly, Harold (WNCP group moderator) has particular settings for the WNCP group: *“Yes, this is the only WhatsApp group…that immediately shows the message on my screen and that also has a different notification sound”.* Moderator John explains what type of specific sound he installed for his WNCP group: *“a special tone, like a foghorn”.* A special notification sound makes that the conversation stands out. This embodies how the meaning of a WNCP group conversation differs from other WhatsApp interactions. Namely, WNCP groups focused on safety are perceived as more urgent than other conversations. Other respondents also installed specific notification sounds for different contacts and contexts. For instance, Harold (WNCP moderator) indicates that messages from his daughter sound differently than other messages.

Moreover, group conversations can also stand out because of the use of a profile picture. Individuals can upload a profile picture to WhatsApp which becomes visible as the thumbnail for one-to-one conversations (in the main interface of WhatsApp). For group conversations, participants can change the profile picture (*group image)*. During the interviews about WNCP, multiple respondents showed us the group conversations on their phone. For many of them, the group image was a logo or image of their group. Moderator Ron proudly explains: *“…We needed a professional logo, and that, together with the municipality, I designed this whole concept”.* By changing the group image, people can make visual distinctions between different contexts. These adjustments in the visible and audible appearance of WhatsApp conversations form material proof of boundary sculpting practices.

Muting particular groups

In contrast to emphasising the importance of particular contexts, users can also reduce the prominence of WhatsApp conversations by muting particular (group) conversations. Each conversation offers the opportunity to mute notifications for eight hours, one week or one year, and this setting can be disabled at any time. When muted, the only indication of new messages is a number badge that becomes visible when WhatsApp is opened. Many of our respondents use the muting setting to manage communication overload and to create boundaries between different (groups of) contacts. Some choose to mute their work WhatsApp group, e.g., Sarah works in a restaurant and mutes the group conversation on days that she is not working. In contrast, Tom (human resources manager) never mutes his work WhatsApp conversations, but mutes his family group. He explains: *"When a picture of my niece is shared again and everyone reacts, I'll easily receive 15, 20, 25 messages… And it so annoying when my phone is buzzing for half an hour".* Even though one-to-one conversations can also be muted, our respondents only mute group conversations because these can more easily create communication overload. Notably, in the WNCP context, muting the WhatsApp group has a detrimental effect on the effectiveness of crime prevention activities. The goal of the groups is to safeguard the neighbourhood by keeping an eye out, and by assisting law enforcement when suspicious activities or emergencies occur. This only works effectively if all participants respond fast, and WNCP moderator Kai explains: *"You want to prevent that people mute the [WhatsApp] group, because then it doesn't work in case of an emergency".*

When dealing with communication overload, individuals devise organising tactics and install distinctive sounds and visuals to visibly and audibly carve out different relational contexts. These practices are all guided by the purpose of reducing pressure while remaining available for particular contexts. However, again, particular knowledge about the functionalities of WhatsApp is required in order to devise messaging management strategies that help individuals to reduce pressure from different contexts. Material barriers function as tools to protect their freedom and autonomy and to prevent an overload of messages from overloading their minds (and lives).

Conclusion: Boundary work as meaningful practices

This chapter explores a variety of boundary work practices within WhatsApp use, and contributes to boundary work literature which aims to understand how individuals deal with technology in managing boundaries between work and personal life (e.g., Duxbury et al., 2014; Jahn et al., 2016; Sayah, 2013; Siegert & Löwstedt, 2019). Our research expands beyond this professional/personal binary and provides an in-depth overview of boundary management strategies in more nuanced relational contexts. We show how people use WhatsApp features to carefully sculpt boundaries between different contexts and to manage absence and presence on a granular level. Boundary sculpting practices are the result of an interplay between knowledge, meaning, and material elements (following Shove et al., 2012). Our analysis presents three conclusions:

First, **everyday practices to demarcate absence and presence are shaped by the meaning attributed to particular relational contexts**. In order to deal with constant networked connections, people engage in purposeful practices of networked absence (Burchell, 2015, 2017). In this process, they make use of *disconnective* affordances (Mannell, 2019). Our research exemplifies how our respondents do this in their WhatsApp use and how the role of relational contexts proves to be crucial. For instance, signal-jamming is often used by respondents in order to be temporarily unavailable for workplace communication. Yet, this strategy is less often used by WNCP moderators because their safety-focused conversations demand constant attention. The meaning attributed to work conversations (being available professionally) is completely different from the meaning of WNCP groups (safeguarding). Moreover, our respondents use silent mode and WhatsApp's last seen setting and blue checks. Different relational contexts require different boundary sculpting tactics to manage presence and absence.

By focusing on boundary work within the use of messaging apps, our research revisits the concepts of permeability, integration, and segmentation (Clark, 2000; Nippert-Eng, 1996a, 1996b). Within WhatsApp, the borders between different contexts are fully permeable and the default is a full integration of contexts. This can be problematic because continuous messaging flows from different contexts cause experiences of stress and communication overload. Our respondents engage in boundary work and decrease permeability between contexts by segmenting messaging flows on a granular level. Individuals put boundaries in place by enabling and disabling particular functionalities and by changing settings for different conversations. More specifically, boundaries materialise in the form of muted conversations, particular sounds, and groups of contacts exempted from the do not disturb mode. These practices require detailed knowledge about WhatsApp features and settings. Thus, our second conclusion indicates that **experienced WhatsApp users have more sophisticated opportunities to sculpt boundaries and to manage communication overload than less tech-savvy users.**

Third, our research highlights how boundary work practices in messaging app use revolve around more than the aim to separate work from private life. Namely, **the ongoing contradictions of messaging practices—always available but always negotiating that availability—affect privacy, freedom, and autonomy in significant ways.** WhatsApp functionalities currently default to visibility in all interactions. For example, they provide information about when users are online and when they read messages. This infringes individuals' privacy, especially if they are not aware of these functionalities (which proved to be the case for some WNCP group participants). Moreover, people are constrained in their freedom when they experience pressure and expectations from the never-ending flow of messages in collapsed contexts (Pagh, 2020; Vitak et al., 2012). More than ever, people are constantly tied to their phones by messaging apps. People can adjust messaging features and tinker with settings, yet, they are limited by the inadequate options offered by messaging apps (particularly for group conversations). This reiterates a crucial point: the default settings of messaging apps take away the user's autonomy to effectively deal with an overload of messages and the collapsing of relational contexts they cause. People would benefit from clearer options for active boundary-sculpting in one-to-one interactions as well as in group conversations in order to safeguard their privacy, freedom, and autonomy.

Limitations and suggestions for further research

The aim to maximise diversity in contexts helped in highlighting overlapping practices and strategies, yet also meant that we did not zoom in on specific groups. Students might employ different strategies and have different reasoning behind their practices than pensioners, or parents of young children. Future research should integrate more contexts, or focus on particular groups. Finally, our results highlight a variety of practices which is not conclusive – e.g., none of our respondents use dual SIM (subscriber identity module) smartphones which might also form an effective tool in boundary work practices.

However, the popularity of messaging apps and other communication services is at present far from waning. In contrast, this research was done before the global Covid-19 pandemic (ongoing from early 2020), which has only accelerated the merging of contexts via technologies. The global lock-down situations caused people to work, educate their children, maintain social ties, and engage in other activities from their homes. It is crucial to understand the effects of blurring boundary practices, because they will become increasingly difficult to sustain and maintain in a post-Covid society. It is likely that the connected flexibility afforded by the use of messaging apps and new communication tools for work, communities, families, and social lives will increase. This suggests that more focused research is needed to fully understand user practices and the boundary work ever present in the use of messaging apps.

Chapter 6

"Even jokes are work-related" Communication privacy management practices in workplace interactions[7]

Introduction

> *"I use many different communication apps on my phone (...) Eh, let's see.. Skype, iMessage, WhatsApp, Facebook, Facebook Messenger, Hangouts, FaceTime, Snapchat, Slack, Telegram, Firechat, Discord, Signal, what else? GoogleDuo, GoogleHallo, GoogleVoice, Basecamp."* (Jay, owner of multiple start-ups)

Jay's quote illustrates how workplace communication can take place via a plethora of digital tools. Whereas this is an extreme example, most people interact with their colleagues and supervisors through multiple digital channels, such as email clients, (enterprise) social media, and messaging apps. Asynchronous communication platforms enable ongoing workplace interactions that can be accessed anytime anywhere. For many employees, especially in office jobs, digital communication platforms proved to be crucial when the global Covid-19 pandemic forced them to work from home. This chapter draws on pre-Covid interviews to provide a sociomaterial understanding of communication privacy management (CPM) practices in digital workplace communication.

As indicated in the introductory chapter, *communication privacy management* (CPM) theory helps to understand how people establish boundaries to manage tensions between concealing and disclosing private and public information (Petronio, 2002). CPM practices are especially interesting in contemporary workplaces because digital workplace communication often happens via personal devices and accounts. This

[7] At the time of printing, this chapter is under revision for *Information, Technology & People.*

chapter explores how employees in different professional roles engage in sociomaterial CPM practices in digital workplace communication and is guided by three research questions.

First, CPM practices in dyadic co-worker interactions, work teams, and supervisor-employee relationships entail variations in risks and privacy considerations (Krouse & Afifi, 2007; Petronio, 2002). The fact that different relations and professional roles bring particular risks informs Research question 1: **How do managers, office employees, service-industry employees, and self-employed professionals engage in CPM practices to manage digital workplace communication risks?** Second, CPM practices are motivated by different criteria (Smith & Brunner, 2017) which I explore via research question 2: **Which core and catalyst criteria inform digital CPM practices across professional roles?** Finally, CPM also takes place within (enterprise) social media interactions (Frampton & Child, 2013; Laitinen & Sivunen, 2020; Snyder & Cistulli, 2020) and therefore I include research question 3: **How do employees manage private information sharing and professional connections via (enterprise) social media and messaging apps in and around the workplace?**

This chapter contributes to the growing body of research about CPM in workplace contexts with a sociomaterial approach to CPM practices. Next, an overview of CPM literature in the workplace is provided as well as insights into the methodological considerations. Afterwards, I present privacy rules and informational boundaries as tangible aspects of everyday work life in the results section, and I identify consequential challenges in the conclusion.

Literature: CPM, workplaces, and practice theory

To adequately explore the practices people employ to manage privacy in digital workplace communication, this section describes the basis of CPM theory. Subsequently, I present existing research about CPM practices in work contexts and introduce practice theory as a conceptual lens for analysing sociomaterial workplace CPM practices.

Communication privacy management (CPM)

Communication privacy management (CPM) theory aims to understand how people actively manage information they consider private (Petronio & Child, 2020). People establish metaphorical boundaries to protect their private information and to manage tensions between concealing and disclosing information. This theory takes into account the inherent dialectic tensions between needing both privacy and openness, and between telling and concealing (Petronio, 2010). In social relations, boundaries are managed by adjusting the transmission and sharing of private information. People regulate the boundaries by deliberating and deciding what private information they disclose or conceal (Petronio, 2002). These boundaries can vary from thick boundaries for a high level of control and many restrictions to access (e.g., for information about sexual preferences) to thinner, more permeable, boundaries for moderate control with few restrictions to access (e.g., for information like age). The level of control varies across situations and can change over time. CPM practices are informed by three core general concepts; *ownership*, *privacy rules* and *turbulence* (Petronio, 2010).

First, *ownership* is based on the prediction that individuals believe that their private information belongs to them. They are the owners of their private information and expect a right to privacy, a right to control what others know about them (Petronio, 2010). The sharing of private information leads to co-ownership, this can happen on a one-to-one basis can also result in collective ownership when more people are involved. CPM investigates flows of private information between and among individuals in order to understand privacy management on individual and collective levels (Child et al., 2012). Individuals have to manage multiple privacy boundaries simultaneously for private and co-owned information (Petronio, 2010).

Second, people control their private information via *privacy rules*. Individuals actively manage rules to determine when, how, with whom and in what way access to private information is granted or denied. In other words, privacy rules determine what a recipient is (not) allowed to do with co-owned information, e.g., the co-owner might be allowed to share information with others or might be expected to keep information to him- or herself. Privacy rules vary across relationships and are influenced by cultural, contextual, and motivational factors. These factors take different forms; *core privacy rule criteria* are stable and predictable, such as cultural influences and societal norms (Petronio & Child, 2020). Privacy rules are also influenced by variable and unpredictable factors, described as *catalyst privacy rule criteria*. For example, situational transformations like getting a divorce can change privacy rules (Petronio & Caughlin, 2005; Petronio & Child, 2020). Core and catalyst criteria provide the basis for how people regulate privacy boundaries in their everyday lives. When information is shared, co-owners need to follow implicit or explicit privacy rules regarding who else they can share information with (*linkage rules*), how much of the information they can share (*permeability rules*), and *"the level of independent judgments the owner allows the co-owner to determine third-party access"* (*control rules*) (Petronio & Child, 2020, p. 77).

Privacy rules are developed on the basis of risk/benefit estimations, people balance the risks and gains of disclosing private information. Petronio (2002) identifies five different types of risks wherein disclosure can lead to high, moderate, or low level consequences. Risks can entail jeopardising the safety of the person disclosing the information or others, being judged differently or discredited due to stigma, loss of face by being embarrassed, relational consequences, and the shifting of roles. Moreover, privacy rules can be singular and individual as well as collective. Collective privacy rules involve multiple boundaries of different people, such as colleagues, family members, or social media contacts. Collective boundary rules thus require coordination between different people, which is often challenging. In collective boundary coordination tensions can arise between privacy rules for individuals versus the entire group (Petronio & Child, 2020).

Third, *boundary turbulence* occurs when privacy rules are violated. Co-owners of private information might not live up to the expectations and violate the privacy rules (deliberately or unconsciously). *"Boundary turbulence occurs when violations, disruptions, or unwanted mistakes are made in the way that co-owners control and regulate the flow of private information to third parties"* (Child et al., 2012, p. 2081). This can happen for singular and for collective privacy rules and often leads to a breakdown of trust between owners and co-owners of information. Boundary turbulence requires people to adjust and recalibrate privacy rules (Petronio & Child, 2020). This can also occur in mediated communication on social media, and research shows that people adjust their privacy management strategies in anticipation of boundary turbulence. For instance, they delete previously shared information to protect their safety and personal identity (Petronio & Child, 2020).

CPM in work contexts

In the workplace, people have to manage personal, dyadic, and group boundaries (Petronio, 2002). Research shows that CPM offers a useful framework to investigate privacy boundaries in the workplace in relation to private information disclosure (Krouse & Afifi, 2007; Magsamen-Conrad et al., 2013; Smith & Brunner, 2017; Steimel, 2021), workplace surveillance (Snyder & Cistulli, 2011; Stanton & Stam, 2003; Watkins Allen et al., 2007), and (enterprise) social media (Frampton & Child, 2013; Laitinen & Sivunen, 2020; Snyder & Cistulli, 2020). These sources inform this chapter's abovementioned research questions about professional roles, privacy rule criteria, and workplace social media use.

Organisational roles and CPM

Work environments require CPM strategies on various levels, private information is disclosed within dyadic co-worker interactions, work teams, and supervisor-employee relationships. Work environments bring particular risks and considerations in CPM strategies for workers at different levels. In open organisational environments, employees are encouraged to maintain permeable boundaries in their relationships. This requires a receptive attitude from all parties involved, e.g., both supervisors and employees need to open up privacy boundaries to enable disclosure between them (Petronio, 2002). Employees differentiate in what types of information they share with whom, they turn to people with more authority for work-related problems, and to peers and co-workers for personal matters. They *"differentiate between levels of information and privacy boundaries"* (Petronio, 2002, p. 171).

Disclosing information to peers at work might involve less risk than disclosing information with a supervisor (Krouse & Afifi, 2007). Steimel (2021) shows how women who experienced pregnancy loss differentiate in their privacy management, they share different parts of their experience with different colleagues on different levels. Most of the respondents felt forced to share some details with their supervisors to account for absence, medical appointments, and needing time off, while they shared the full story voluntarily with their closest co-workers. Workplace roles enforce asymmetric communication privacy boundaries, which is visible in how their respective roles presented these women with coercive linkage rules. Moreover, in work environments disclosing information brings specific risks when it comes to professional roles. For instance, when a supervisor discloses private information with an employee who deems this inappropriate, the supervisor’s professional role can be compromised (Petronio, 2002). For Steimel’s (2021) respondents, the information that they share about their miscarriages can also present a stigma risk, because miscarriages concern a sensitive and potentially stigmatizing topic. As indicated in the introduction, the significance of professional roles in workplace CPM strategies informs the first research question: How do managers, office employees, service-industry employees, and self-employed professionals engage in CPM practices to manage digital workplace communication risks?

Disclosure in the workplace

Workplaces can form a site where forced disclosure of information occurs, this happens when employees are exposed to digital workplace surveillance, such as the monitoring of emails, work devices, browsing practices, software uses, and calendars (Stanton & Stam, 2003; Watkins Allen et al., 2007). Employers take ownership of the information of their employees and workplace surveillance amplifies power inequalities between workers subjected to digital monitoring and superiors enforcing these practices. This leads to contested boundary ownership, because employees lack the power to fully engage in boundary management processes when they are subjected to workplace surveillance (Watkins Allen et al., 2007). Furthermore, the monitoring of email violates email privacy rules and leads to a decrease in trust in supervisors and, consequently, affects employee-supervisor relationships negatively (Snyder & Cistulli, 2011).

Apart from forced disclosure of information, employees also actively manage voluntary disclosure of private information at work (Smith & Brunner, 2017). Organisational culture is a core criterion in the development of privacy rules in the workplace, close-knit versus closed-off cultures elicit different privacy rules. Relational considerations form another core criterion, employees share information to foster personal connections in which they base their considerations on trust. Also, catalyst criteria for privacy rules in the workplace are based on a desire for feedback, and on risk/benefit considerations around the fear that their private information would harm their reputation or alienate co-workers (Smith & Brunner, 2017). Here, communication privacy management is informed by risks of losing face and relational consequences (Petronio, 2002). Smith and Brunner’s (2017) emphasise the need to study privacy practices in different professional roles, to find if supervisors’ privacy considerations are influenced by the same criteria as those of employees. Therefore, I pose the second research question: Which core and catalyst criteria inform CPM practices across different professional roles?

CPM in (enterprise) social media use

In many workplaces, colleagues interact face-to-face as well as via digital channels. Covid-19 presented a shift towards more digital interactions as many workers in many countries were forced to work from home. Apart from email, people can communicate via (enterprise) social media, online collaboration tools, videoconferencing, and messaging apps. Digital workplace communication provides employees with opportunities as well as challenges they need to manage in their everyday work life. Social media can present CPM dilemma’s when employees receive friend requests from their colleagues (Frampton & Child, 2013). Because public social media are of personal nature, employees have to re-configure their privacy rules and decide whether they want to provide their colleagues with access to the private information they share on social media.

Almost all employees accept friend requests, and only some experience this as a privacy dilemma and adjust their privacy rules for their social media content. For the latter group, Facebook friend requests can cause a form of turbulence when experienced as a privacy invasion or surveillance attempt. Similar to private information disclosure in the workplace, organisational culture also informs privacy rules around social media use. According to Frampton and Child (2013), Facebook-related CPM practices of employees were influenced by organisational privacy culture, employees who accepted friend requests came from organisations with less of a privacy culture and organisations with stricter privacy regulations were home to employees not responding to friend requests. Moreover, stricter organisational privacy orientations led to more restrictive individual privacy rules (Frampton & Child, 2013). Interestingly, social media relationships in the workplace can lead to higher levels of trust between supervisors and employees, which is also influenced by organisational culture and self-reported social media efficacy (Snyder & Cistulli, 2020).

Enterprise social media (ESM) are *"multidimensional web-based communication tools that allow collaboration and information sharing"* (Laitinen & Sivunen, 2020, p. 642). Whereas ESM allow employees to build profiles, post information, and interact, they differ from public social media in scope (often limited to the company), audience (only colleagues), and offer collaboration opportunities. Laitinen and Sivunen (2020) show that employees' information sharing practices are based on personal, technological, and organisational considerations. ESM encourage social interactions; however, they were not often used to share private information. Employees preferred not to share private information via ESM, calculating risks for their professional role as well as online safety risks. In addition, employees felt uncertain about the nature and breadth of their ESM audience. They feared a loss of face when sharing unsuitable or too much private information to a larger audience.

For these respondents, organisational culture and organisational norms proved to be core criteria in their CPM practices (Laitinen & Sivunen, 2020). Snyder and Cistulli's (2020) findings inspire CPM research about personal social media use for digital workplace communication and the work of Frampton and Child (2013) and Laitinen and Sivunen (2020) shows that it is important to take ESM into account when investigating workplace CPM practices. In addition, WhatsApp is often used in Dutch workplaces. Messaging apps overlap with social media by enabling users to engage in interactions, create profiles, and share pictures and videos (Wei, 2020) and therefore, they are also included in the third research question: How do employees manage private information sharing and professional connections via (enterprise) social media and messaging apps in and around the workplace?

A practice theory approach to CPM

This chapter aims to understand the sociomaterial nature of CPM practices in workplace communication (see Chapter 2 for an explanation of a sociomaterial practice theory approach). With regard to digital workplace communication, the competence, meaning, and material dimension of Shove et al.'s (2012) practice theory model is applied in the following manner: competence concerns knowledge about how to navigate and use different communication technologies, and an understanding of organisational culture and norms. Second, meanings range from efficiently getting work done to maintaining personal connections. Finally, materials refer to the objects, or *things* involved in practices – such as smartphones, laptops, digital interfaces, but also the (bodies of the) employees engaging in these practices. In this chapter, the interplay between these three elements provides a sensitising concept in the analysis of workplace communication CPM.

Research method: Workplace interviews

I conducted semi-structured in-depth interviews and analysed these inductively via a constructivist grounded theory procedure (Charmaz, 2014; Corbin & Strauss, 1990). The methodological details are included in Chapter 2, and the interview guide in Appendix 6. The respondent overview in Appendix 2 also indicates the professional role and types of workplaces of the 16 participants. Respondents discussed how they use public social media, enterprise social media, and messaging apps. The results section presents an in-depth understanding of the recurring themes around CPM and digital workplace communication via WhatsApp and other (enterprise) social media channels (see Appendix 13 for the codebook).

Results: CPM challenges across professional roles

In order to explore the differences in CPM practices across different professional roles (RQ1) this section provides insights in the themes that proved to be particularly meaningful for managers, office employees, self-employed professionals, and service-industry employees. I highlight which specific criteria influence their practices (RQ2). The analysis also provides insights in more universal themes which will first be presented. Table 2 shows which themes are meaningful for respondents in particular professional roles, and which themes are prevalent for all respondents. Since social media is paramount to digital workplace communication, RQ3 is answered throughout the results section. Moreover, answers to all research questions are synthesised in the conclusion.

Table 2: Recurring CPM themes

<table>
<tr><th>Managers</th><th>Office employees</th><th>Service-industry employees</th><th>Self-employed professional</th></tr>
<tr><td>Private information considerations</td><td>Professional nature of communication</td><td>Turbulence workplace communication</td><td>Flexible distributed communication</td></tr>
<tr><td>Professional role tension</td><td>Company culture</td><td>Social media face risk</td><td>Social media business</td></tr>
<tr><td colspan="4">Strict boundaries private/professional information</td></tr>
<tr><td colspan="4">Permeable boundaries private/professional information</td></tr>
<tr><td colspan="4">Safety risks</td></tr>
</table>

From *strict to permeable boundaries* and *safety risks*

The themes *strict boundary private/professional information* and *permeable boundaries private/professional information* seem to indicate that there are two exclusive attitudes towards disclosing private information. However, the fact that both of these themes were meaningful for respondents across professional roles illustrates how CPM is an active process in managing the tensions between concealing and disclosing information and between privacy and openness (Petronio, 2010; Petronio & Child, 2020).

Phones proved to be material dimensions of strict privacy boundaries. Kenneth, manager in a zoo, provides an interesting example of how different phones embody different information flows with different levels of disclosure. When Kenneth is at work, he makes use of three devices. The first device is his private smartphone on which interactions take place with personal connections. He also carries a basic phone for workplace communication which is purely used for professional communication in the workplace. The third communication device concerns a *“portable radio-telephone with an emergency channel through which you can reach all crucial parties…these we use in case of emergency for really fast communication”.* This is a unique example, but it illustrates a strict material separation between different information flows, with different meanings: social life, professional interactions, and emergency information respectively. Each device also requires different know-how of how to operate the devices and an understanding of the implicit rules about when (not) to use them.

In contrast to Kenneth’s phones enacting material separation, phones can also form tangible proof of permeable privacy boundaries. Lauren (self-employed professional) also has a separate work phone, however, this work phone enforced a boundary she felt was too strict. She preferred to integrate private and professional communication on one device: “*I noticed that I keep track of my private phone better, so I basically transferred all WhatsApp conversations with colleagues to my private phone… Yes, [I did this] because I missed messages, especially when it happens in the weekend*”. Lauren wants to keep up to date via her private smartphone, which is visible in how her WhatsApp interface includes private as well as professional interactions. Yet, while she often discloses private information to her colleagues she prefers to do so face-to-face, supporting existing research (Laitinen & Sivunen, 2020).

Permeable privacy boundaries are sculpted through particular uses of digital communication tools. Some platforms allow for a separation of messaging streams, e.g., workplace communication tool Slack (which can be considered enterprise social media, see Willis, 2019) enables users to create different channels. Lara (office employee) uses this feature: “*I also send private messages via Slack, with some direct colleagues I share personal things. For instance, we have a group of colleagues we do sports with, and that is just a channel within our company Slack group*”. Lara manages asymmetric privacy rules as she differentiates between groups of colleagues. Her CPM practices display the know-how of managing different interactions which each have a different meaning and embody different privacy rules. As such, Lara’s practices are similar to those of Steimel’s respondents (2021).

Jay (self-employed professional) also provides an example of how privacy rules are embodied by digital flows of information. He describes his private information sharing practices: *"In January, my son was born, but if people say something like: 'Hey, I cannot find any pictures of your child on Facebook, please send me a one'. Well, I'd never do that because Facebook or Google shouldn't be able to possess my pictures. So I'll use Signal or iMessage or something".* This example shows how Jay establishes thick boundaries around pictures of his son, in order to have a high level of control over information (pictures) that he deems too sensitive to share via particular channels. Pictures of his son form a material indication of information with a sensitive nature and the meaning of different platforms bring different connotations of safety. Signal or iMessage embody trustworthy platforms, whereas Facebook and Google cannot be responsible co-owners of Jay's private information. Apart from illustrating how CPM practices materialise in using different communication services, Jay's considerations are also influenced by privacy rules.

Specifically, Jay touches upon a privacy rule related to social media that many respondents discussed, namely the safety of their online private information. Safety risk forms a core privacy rule criterion (Petronio & Child, 2020). Respondents fear that privacy rules are not respected by commercial platforms and that this will lead to boundary turbulence, a risk calculation also described by Laitinen and Sivunen (2020). Victor (manager) explains: "*All the information that WhatsApp and Facebook combined so far is already dangerous in my view, but if it falls into the wrong hands because of hacks, hackers can blackmail or destroy basically everyone"*.

Commercial organisations are seen as anonymous co-owners of data, which are difficult to steer in their adherence to privacy rules. Privacy protection techniques form tangible tools to safeguard the privacy of private information, however, these require technical knowledge. This is illustrated by Erik (office employee): *"On all platforms I'm using online, whether it's OneDrive, my email, Twitter or Facebook, I've set-up two-step verification. Because I do not want anyone to steal my data".* By using two-factor-authentication, Erik uses his tech savviness to establish a thick boundary around his digital private information. Whereas online safety risks were mentioned by all respondents, not all of them respond to risks as actively as Erik. Most explain their response to safety risks as limiting the disclosure of private information via digital channels. However, the practices described in the next section indicate that, regardless of safety risks, respondents often engage in private interactions via digital communication platforms.

Managers: *Private information considerations* and *role risks*

Digital workplace communication often takes place on the brink of the professional and personal realm, which leads to private information considerations. In many Dutch workplaces, messaging service WhatsApp is used for everyday communication. As Mark (manager) explains: “*WhatsApp has a character of personal communication. It is not email, it is not a letter, as far as people still send letters, WhatsApp has an informal basis”*. Moreover, Victor (manager) feels uncomfortable with the physical location of WhatsApp messages: *“For me, WhatsApp is more located in my private environment. And I feel a bit uncomfortable that some professional contacts are situated within my private WhatsApp contacts”.* Most public and enterprise social media provide opportunities in which contacts are visible and allow for the targeting of specific audiences. As Victor indicates, messaging apps like WhatsApp provide no tangible distinctions between conversations. Instead, all interactions are located in one digital interface, and know-how of WhatsApp features is required to create audible and visible distinctions (see also Chapter 5).

Workplace WhatsApp group chats are located in between conversations with personal contacts, which increases the risk of boundary turbulence when information is accidentally shared in the wrong interaction, when messages are forwarded to others without the consent of the sender, or when respondents share content that others deem inappropriate or risky. Many respondents provide examples of how the informal character of WhatsApp goes hand in hand with the sharing of personal content in work WhatsApp conversations. Apart from sharing work-related content, respondents received personal experiences (such as holiday pictures), opinions, pictures (e.g., party pictures or snapshots of pets), memes, and viral videos. Whereas all respondents have to navigate the benefits and pitfalls of personal disclosures in work WhatsApp groups, this especially creates challenges for managers. As Kenneth (manager) explains, the private content disclosed by his employees on WhatsApp can change the perceptions individuals have about their colleagues:

> *"My colleagues also had a group chat for fun where they discussed topics that were totally unrelated to work…This might influence how I see my colleagues because I get insights into how they think about certain things and how they communicate and how blunt they are, how female unfriendly, or discriminatory, or racist. Therefore, I left the group chat."* (Kenneth, manager)

His employees felt comfortable with disclosing their personal opinions with their co-workers and manager and maintained a permeable boundary. However, for Kenneth, the pictures, statements, and fun content like memes formed material indicators of attitudes and private identities of his employees. Therefore, he left the group chat in anticipation of risk for his employees. These risks include that he would unwillingly stigmatise his employees – he feared he would judge them differently because of what they disclose, or that his employees would regret what they shared with him, or that they would alienate him. By removing himself from the group chat, Kenneth re-establishes a collective privacy rule for his employees towards himself as a supervisor in order to prevent boundary turbulence and risks of stigma, loss of face, or alienation (Petronio, 2010; Smith & Brunner, 2017). This shows that Kenneth's CPM considerations are based on different criteria than those of his employees (answering a question posed by Smith & Brunner, 2017). Social media and the blurring of boundaries between personal and professional conversations present managers with challenges wherein they have to safeguard the privacy of their employees but also their own professional role.

In his discussion of WhatsApp use, Kenneth also touches upon another risk. With one of his employees, a professional WhatsApp interaction changed into a conversation with disclosures about their private lives; *"And now I notice that I find it harder to maintain, eh, to be stricter with her".* Kenneth experiences role risk (Petronio, 2002) because his supervisory role shifts when he perceives his employees differently. While his private disclosures via social media can increase trust (Snyder & Cistulli, 2020), the risk of shifting roles might motivate Kenneth to enforce stricter private information boundary rules towards his employees.

Having experienced boundary turbulence and enforced disclosure of private information in other workplaces in the past, Lea (manager) decided to maintain strict privacy rules in her current supervisory role. She refrains from disclosing private information and interacting via social media with her employees. She indicates that being a manager brings role risks: *"I deliberately decided that I don't want to, pour my heart out or anything, that can make you vulnerable as a supervisor. Especially because you have to maintain some distance in supervising".* The examples of managers Kenneth and Lea confirm how CPM practices are informed by calculating risks for their professional (Laitinen & Sivunen, 2020). CPM practices of managers highlight how the blurring of boundaries between digital private and professional communication forms a catalyst privacy rule criterion. This criterion is accompanied by more stable criteria, specifically, role risks, face risks, and stigma risks challenge individual as well as collective privacy.

Office employees: *professional nature of communication* and *company culture*

For most office employees digital workplace communication is of professional nature. Michael (office employee) indicates: *"At least 90% of the content of our WhatsApp conversations is related to work".* Similarly, Andrea (office employee) describes: *"It is very formal...Sometimes jokes occur, for instance when someone loses a prospective case, a colleague can say 'a glass of whiskey, and you'll be over it'. So, even jokes are work-related".* Workplace surveillance forms a catalyst privacy rule criterion that motivates employees to limit digital workplace communication to professional content. This is a catalyst criterion because it only becomes tangible when an employer acts upon findings of the monitoring practices. This makes the nature of workplace surveillance opaque and uncertain, especially because most workplaces lack transparency in what, who, and when they monitor digital practices. Lara (office employee) anticipates workplace surveillance, and therefore, she is careful in what she shares in digital workplace communication: *"Well, I try not to…eh, to gossip, because you know that there is always someone who can read it. So, I will not talk about colleagues on Slack, I won't".* In order to avoid enforced disclosure of information via workplace surveillance (Watkins Allen et al., 2007), Lara constructed a privacy rule refraining from disclosing potentially risky content via Slack.

Company culture proved to be a core privacy rule criterion for (enterprise) social media. Organisational practices create the expectation that digital workplace communication has a professional character. For all office employees, strict privacy rules within the company influenced their individual CPM practices, this confirms existing research (Frampton & Child, 2013). Moreover, company culture also establishes expectations around participation in digital workplace communication. Tom (office employee) explains *"it is expected [that he joins a departmental WhatsApp group]...I don't know how people will react when I suddenly leave the conversation. There are bound to be questions...And if I provide a good reason, they'd understand. But then I'd miss the fast communication and updates".* Tom does not mind the implicit obligation to join the departmental WhatsApp conversation, because he enjoys the benefits of it. For Tom, the WhatsApp group chat embodies an efficient and desirable part of his digital workplace communication.

However, other employees might not feel comfortable with such communication practices that take place in between their private interactions, but company culture can make them hesitant to leave a WhatsApp group chat. This shows how office employees often automatically become part of collective communication practices with collective privacy rules, over which they lack control and autonomy. In addition, company culture can also establish when interactions can take place. While Erik (office employee) describes his company culture as a hard-working highly motivated and flexible environment, there are unwritten rules about the timing of digital communication. Vacations are visible to everyone in their enterprise social media, and it is considered inappropriate to reach out to colleagues when they are on holiday: *"WhatsApp is a no-go. Nobody does that so you're not going to try if someone reacts. That's just a no-go".* Similarly, while Slack channels are often used during evenings in Lara's workplace: *"It is common that people don't send messages during the weekend".*

For office employees, company culture influences privacy rules around what to disclose and to conceal in digital workplace communication, and also prescribes how and when (not) to interact. Company culture forms a core privacy rule criterion for most respondents but takes most tangible form for office employees. For them, company culture determines the meaning of digital workplace communication as professional, it demands particular knowledge of the dos and don'ts around disclosing information. The interface of the platform, Internet connections, the communication device, and the employees and their colleagues make up the material dimensions of CPM practices.

Service industry employees: *turbulence workplace communication* and *social media face risk*

Service industry employees are different from most other respondents because their work does not take place behind a computer or laptop, and workplace communication serves a practical purpose. Workplace communication takes place via messaging apps and a few official emails, it is less dispersed for service-industry employees than for the other groups of respondents. In the interview with three restaurant employees, they describe how their work WhatsApp group chat is used almost every day and contains a mix of practical information (such as scheduling requests, new menus, workday updates) and fun content (party pictures of colleagues, jokes, birthday wishes). This mix goes together with unwritten rules about what is and what is not appropriate content, and creates particular risks related to the technical features of messaging apps. From all groups, the service-industry employees displayed the most concern about boundary turbulence, this forms a core privacy rule criterion for their CPM practices:

> *"There are things I don't share via social media or WhatsApp, things that I just don't want to be visible somewhere, that someone can actually show it to someone else…Because when you tell something face-to-face, they can share it with others, but it is not written in black and white."* (Jennifer, service industry)

For Jennifer, digital communication poses a greater risk of the violation of her linkage and control privacy rules. When she makes someone co-owner of her private information in a face-to-face context, she anticipates that her information might be shared with others and is willing to take this risk. However, a digital interaction forms a material risk that amplifies the breakdown of her privacy rules. A conversation saved in a digital location becomes a tangible object which can easily be shown to others or forwarded via communication platform features. Jennifer has knowledge about boundary turbulence risks and the material dimensions of conversation contexts determine that face-to-face interactions have a different meaning for her than digital interactions.

The respondents describe how most of their colleagues are also connected via social media. This displays a permeable boundary between work and private life, and between private and professional information flows. This brings particular risks for service-industry employees. Similar to the findings of Smith and Brunner (2017) about face-to-face disclosures, the close-knit company culture in their restaurant leads to permeable privacy rules influenced by risks of losing face (Petronio, 2002) when they share content that can harm their reputation. Sara (service-industry employee) describes how a colleague shared a video on Snapchat (a messaging app wherein pictures and videos disappear after a set amount of time) wherein he was undressing himself in a bar while dancing with a beer in his hands. Someone took a screenshot of this Snapchat video and shared this with other colleagues via social media. Sara explains the risks for her colleague: *"You know, the service industry is a bit looser in that sense, but what if you want apply for a business job, or you want to be a supervisor or something? That is risky".* Upon which Sara's colleague Emily responds: *"Yeah, but now as well, the owner of our restaurant also addressed him about this, she said: 'You are the face of our restaurant, and it is just weird that you expose yourself on social media'".*

This example shows how informal social media interactions among colleagues can lead to boundary turbulence, the colleague trusted his Snapchat contacts to respect his linkage rules (Petronio & Child, 2020). The disappearing image should have prevented others from forwarding of the footage, however, one of his contacts violated his linkage rules and changed the ephemeral video into a lasting image which was then forwarded to others. This led to a breakdown of trust between the sender and the receiver of the video, which in turn led to a loss of face for the employee. Not only his reputation was harmed, but also relational risk occurred because he alienated his supervisor. Such incidents can enforce a recalibration of privacy rules (Petronio & Child, 2020), influenced by boundary turbulence as a catalyst privacy rule criteria and relational considerations and face risk as core criteria (Smith & Brunner, 2017).

Self-employed professionals: *flexible distributed communication* and *social media business*

The self-employed respondents all work in the start-up industry, and they experience different work cultures and digital workplace communication practices than the other respondents. Their work is characterised by dispersed and virtual teams, international collaborations, and communication via many different channels. Jay (self-employed professional) explains the benefit of asynchronous communication platforms: *“I run a business with someone in the US, and I’m involved with a couple of companies as a coach and commercial mentor, and these are spread all over the world, so it is easier to communicate via tools like this”.*

The CPM practices of self-employed respondents like Jay need to be intricate because much of their work takes place via digital communication platforms. For them, the meaning of digital workplace communication is closely intertwined with flexible distributed communication which materialises in a variety of messaging flows across devices and contexts which requires detailed know-how about different platforms. The fact that a lot of collaborations take place online in a field of work based on ideas and innovating, brings particular risks. For Ciara (self-employed professional), her privacy rules are influenced by protecting business information as a core criterion: *“Because we’re doing innovation, and a lot of these projects take at least a year to develop. So, before they are launched, the competition cannot know what is happening”.*

Another theme that is key to the work of the self-employed respondents, is that most use public social media for business purposes. For instance, Marcus (self-employed professional) explains that his grocery delivery start-up uses WhatsApp as the main communication channel with customers. Furthermore, Jay (self-employed professional) interacts with his professional relations via different channels, and he uses personal accounts in this process. He explains: *“For me, there is only a* *very thin boundary between what is business and what is private".* Whereas Jay does not experience privacy dilemma's in using personal social media for professional purposes, for Ciara this presents a privacy invasion. She explains how her work enforced a shift from personal social media uses to using it for business purposes. She currently uses Snapchat, Facebook, and WhatsApp for communication within different projects. For her, this forced blurring of boundaries between personal and professional networks feels like boundary turbulence. Ciara's experiences echo the results of Frampton and Child (2013) who describe how Facebook friend requests can be perceived as privacy invasion or lateral surveillance attempts. Upon the question how she responds to social media friend requests from business relations, Ciara answers:

> *"That would disturb me, because I don't like friend requests [from business relations] …For me Facebook should be a completely personal space. And I have quite some people there from my work and I don't like it because it's my personal stuff and I try to keep it very separate. Like, I don't enjoy mixing these things too much."* (Ciara, self-employed professional)

Because Ciara feels obliged to follow the work culture in the start-up industry, she maintains more permeable privacy rules than she feels comfortable with. Ciara's CPM practices are characterised by privacy rule turbulence, and her personal social media accounts form tangible material locations where tensions arise between different contexts for which she wishes to maintain different privacy rules.

Lauren decided to avoid such tensions and established strict privacy rules around her social media: *"On Facebook, I restricted, eh, only my friends can view my page, and others who are not my Facebook friend can only view my profile picture".* Lauren's work takes place in a field where flexibility and the merging of contexts determine the work culture. However, the personal nature of social media is a core privacy rule criterion for her and therefore, she maintains strict boundaries to protect her private information on social media. Self-employed professionals do not have to adhere to organisational norms and obligations, yet, the flexible, distributed, and digital nature of their work demands permeable boundaries between private and professional information and social media accounts. Jay, Marcus, Ciara, and Lauren provide examples of different ways to manage these expectations and to find a balance between the meaning they ascribe to digital workplace communication, and the flexible meaning that is common in their start-up industry.

Conclusion: Intangible and fluid CPM practices

By drawing on interviews about CPM practices of employees in digital workplace communication, I have noted several key issues for managers, office employees, service industry employees, and self-employed professionals. The sociomaterial CPM practices in different professional roles (RQ1) and in social media use (RQ3) are influenced by core and catalyst privacy criteria (RQ2). This discussion first addresses privacy rule criteria, after which the differences across professional roles, the role of social media, and the materiality of digital workplace communication are discussed. In answering the research questions, I draw general conclusions and provide some practical suggestions for the digital workplace. While this chapter draws on pre-Covid-19 interviews, the conclusions and suggestions address topics prevalent in workplaces and working-from home situations more generally.

The respondents discussed the criteria on which they base their CPM rules around private information disclosure. Some of these are addressed in existing research, and some can be considered novel criteria. For the respondents, core privacy rule criteria proved to be the risk of a loss of face, stigma, the shifting of professional roles, and relational consequences (Petronio, 2002). Moreover, online safety risks prevented them from sharing private information via digital channels (Laitinen & Sivunen, 2020), and company culture influenced their CPM practices (Smith & Brunner, 2017).

Apart from these established stable and predictable criteria, the respondents also based collective privacy rules on the protection of business information, and individual privacy rules on the personal nature of social media. These two core criteria led to establishing strict privacy rules. In addition, strict privacy rules were also established on the basis of unpredictable and variable catalyst privacy criteria. Boundary turbulence in digital workplace communication and the blurring of boundaries between private and professional interactions form catalyst privacy criteria leading to strict privacy rules. Finally, the anticipation of workplace surveillance also forms a catalyst privacy criterion. These catalyst privacy rule criteria are characterised by the fact that they start to matter when an event or experience makes them tangible. **The intangible nature of CPM practices instigates the need for employees to consider the risks of disclosing private information carefully.**

The practice theory approach helped to highlight how digital workplace communication has a different meaning for our different groups of respondents, and how professional roles lead to particular risks and dilemmas in CPM practices across professional roles (as indicated by Petronio, 2002, and Smith & Brunner, 2017). The CPM practices of managers, office employees, service-industry employees, and self-employed professionals revolve around different challenges and issues. The CPM practices of managers are challenged by the blurring of boundaries between professional and private interactions, instigated by digital workplace communication with an ambivalent meaning that is partly taking place in informal contexts. Managers feel they risk their professional role. Whereas some (would) like to engage in the disclosure of private information to their employees, they fear that this will complicate their professional standing and how they perceive their employees. For office employees, workplace communication has a professional meaning. Their CPM practices about what, how, and when to communicate are highly influenced by company culture, which can bring obligations through collective privacy rules that enforce permeable individual privacy rules.

For service-industry employees, boundary turbulence proved to be something they anticipate in a work context where personal social media and professional communication are intertwined. Their digital workplace communication is as close-knit and permeable as their company culture. Self-employed professionals manage the boundaries between personal and professional communication, which for some creates boundary turbulence. In their field of work, it is common to use personal social media accounts for digital workplace communication characterised by flexibility. Our research supports that there is fluidity in how people manage privacy rules, and in order to prevent privacy break-downs and boundary turbulence in and around the work context, **employees and managers should actively engage with their colleagues, and professional relations to coordinate mutually understood privacy rules.**

Furthermore, by integrating different types of digital workplace communication, it became clear that social media poses dilemmas and challenges to most respondents. While international connections, asynchronous interactions, and prompt reactions are presented as benefits of social media use for workplace communication, there were no indications that trust between supervisors and employees would increase by social media connections – as Snyder and Cistulli (2020) found. Instead, social media poses dilemma's (Frampton & Child, 2013) informed by role, face, and turbulence risks. All respondents feared online safety risks, echoing Laitinen and Sivunen's findings (2020). And more specifically, managers fear that self-disclosure of private information towards employees leads to a loss of face, self-employed employees experience boundary turbulence when they use personal social media accounts for professional communication, and service-industry employees fear risks of losing face and alienating professional relations when social media interactions affect their professional reputation. For our respondents, the risks of blurring the boundaries between private and professional social media use seem to outweigh the benefits. Therefore, I suggest that **employers carefully consider information about their employees they receive via social media, be it directly or indirectly as strictly personal, and respect the boundaries between social media disclosure and professional roles.**

Finally, phones, computers, and platform interfaces form tangible material objects which embody digital workplace communication practices. While these take many different forms, they are characterised by multiplicity. Almost all respondents shared how they have to juggle different information flows and devices, which can lead to stress and boundary turbulence when conversations and requests from different contexts intertwine. This chapter shows that the dilemma's identified in existing research focusing on social media and face-to-face disclosure (Frampton & Child, 2013; Smith & Brunner, 2017), are amplified when the scope is broadened to include different forms of workplace communication. For managers and office employees, it would be best if companies streamline the internal communication and provide guidelines on when to use which platform. Naturally, individuals should be able to exercise their autonomy in their everyday work interactions, but also need the opportunity to fall back on demarcated communication flows. My findings understate that company culture influenced the workplace communication practices and privacy rules of the respondents, echoing existing research (Frampton & Child, 2013; Laitinen & Sivunen, 2020; Smith & Brunner, 2017). This indicates that **employers can play a crucial role in reducing boundary turbulence and stress of their employees by providing clear communication guidelines.**

Limitations and suggestions for future research

Whereas my findings study provides a helpful starting point for understanding CPM practices in digital workplace communication, the interview sample is relatively small and limited to a Dutch context. Future research can help to understand if the findings can be translated to different countries, and other work contexts. Moreover, the exploratory nature of the interviews allowed for respondents to discuss all the workplace communication tools they use. However, the Covid-19 pandemic instigated a surge in the development of online collaboration tools which might have changed digital working practices. Our research does not include tools like Microsoft Teams, Cisco WebEx and Zoom, which increased in popularity and penetration rates in the course of 2020. Future research should therefore widen the scope of digital workplace communication tools.

Finally, this chapter touches upon individual as well as collective information and CPM practices. For instance, individual and collective privacy rules become clear in Ciara's concerns about disclosing sensitive business information. For an adequate understanding of privacy management, controlling individual and collective information deserves more in-depth attention in future research – something also argued by De Wolf et al. (2014) who demand more attention for group and individual privacy management in social media use.

PART 3

Practices of control in intimate contexts

Chapter 7

"I believe that you're part of a huge Google A/B test" Privacy concerns around smart speakers[8]

Introduction

> A man in sweatpants and socks enters the kitchen and says:
> *"OK Google. Play the morning playlist."*
> A Google Home device on kitchen counter lights up and
> replies: *"OK, playing morning playlist."*
> Soft music starts to play.
> Man: *"OK Google, play music in all rooms."*

This is a fragment from a Google Home commercial about a family (Peek of the Net, 2017). Google Home devices are integrated into this family's morning routine and are consulted by all family members for travel updates, homework queries, calendar items, and traffic information. This commercial illustrates how household Intelligent Personal Assistants (IPAs), also referred to as smart speakers, are becoming part of everyday life (for an explanation of IPAs, see the introductory chapter). The US is forerunner in adoption with nearly 90 million US adults using household IPAs in January 2020 – 34.4% of all US adults (Kinsella, 2020). In 2018, household IPA ownership in Western Europe amounted to 22.4% of Internet users in the UK, compared to 17.2% in Germany and 14% in France (McNair, 2019). The most popular household IPAs are Amazon's Echo devices, Google's Home devices, and Apple's HomePod (Perez, 2019).

[8] This chapter is a slightly altered version of Mols, A., Wang, Y., & Pridmore, J. (2021) Household Intelligent Personal Assistants in the Netherlands: Exploring Privacy Concerns around Surveillance, Security and Platforms. Accepted for publication in *Convergence.*

The integration and normalization of household IPAs has led to concerns in relation to the devices *listening in* (Lau et al., 2018), the *platformisation* of the home, and security (Lei et al., 2017). Researchers emphasise that more awareness about the privacy implications of household IPA use is required (Chandrasekaran et al., 2018; Lutz & Newlands, 2021; Manikonda et al., 2017). Our mixed methods research is based on a survey and focus groups and explores privacy concerns of potential users in the Netherlands. We provide insights about a continental European population that is culturally distinctive from previous studies which mainly research US and UK populations (Huang et al., 2020; Liao et al., 2019, Manikonda et al., 2017). This chapter also focuses on a population just at the cusp of normalizing these devices within the home – our research took place in Spring 2018 whereas after the introduction of the Google Home in November 2018, household IPA ownership grew from 5% of all Dutch households in 2019 to 19% in April 2020 ('Slimme speaker verovert huiskamer consument', 2020; 'Slimme Speakers in Half Miljoen Huishoudens', 2019).

A growing body of research about household IPA use discusses privacy concerns, yet, only few researchers differentiate between different types of concerns (Lutz & Newlands, 2021; Manikonda et al., 2017). Because privacy concerns are not uniform, we distinguish between surveillance, security, and platform-related issues which are presented in the literature section. Subsequently, our results section contributes to a multidimensional understanding of household IPA privacy concerns in which we highlight the role of affordances. Our survey examines to what extent multidimensional privacy concerns are influenced by their familiarity to the Internet, digital literacy, general privacy concerns, and phone IPA use.

The analysis is guided by RQ1: **Which factors influence household IPA privacy concerns in the context of surveillance, security, and platforms?** Subsequently, the results from our focus groups are used to explore the role of affordances in order to answer RQ2: **What role do affordances play in household IPA privacy concerns in the context of surveillance, security, and platforms?** We draw out a nuanced understanding of privacy perceptions around household IPAs, indicating how these smart home technologies raise concerns about privacy, surveillance, device security, everyday behaviour, and platform transparency.

Literature: Household IPAs, privacy, and affordances

Household IPA use goes hand in hand with everyday considerations around user privacy. Researchers suggest that more awareness of privacy threats of household IPAs and knowledge about protective practices is needed (Malkin et al., 2019; Manikonda et al., 2017). However, others indicate that awareness not always leads to privacy protecting practices (Huang et al., 2020; Lutz & Newlands, 2021). It might be the case that some users of household IPAs accepted these privacy risks or became fatalistic or apathetic towards privacy concerns (Lau et al., 2018; Lutz & Newlands, 2021; Pridmore et al., 2019). Nevertheless, privacy concerns have had a demonstrably weakening effect on motivations for household IPA use (McLean & Osei-Frimpong, 2019). Recent studies including non-users suggest that privacy concerns can also lead to a lack of trust in household IPA platforms, and consequently, form a reason not to use a household IPA (Lau et al., 2018; Liao et al., 2019). Therefore, it is important to provide a better understanding of the foundations of privacy concerns and insights into diversity within these. Following Lutz and Newlands (2021) and Manikonda et al. (2017), we use a multidimensional conceptualization of household IPA privacy concerns. We differentiate between surveillance, security, and platform concerns: Surveillance concerns revolve around household IPA devices being perceived as surveilling agents listening in on users; security concerns focus on device security threats; and platform concerns regard issues around data collection, processing and sharing by IPA platforms.

Privacy as a multidimensional concept

Surveillance, security, and platform-related privacy concerns each focus on different aspects of household IPA use. As discussed in the introductory chapter, privacy is a fluid and abstract concept, loaded with moral considerations. Privacy is approached as a multifaceted concept and household IPA concerns are viewed through the lens of Koops et al.’s (2016) nine types of privacy. *Information privacy* is paramount to household IPA privacy concerns because these revolve around the collection of and access to user data and personal information. In the context of household IPA use, information privacy is intertwined with three other types – namely *communicational, spatial,* and *intellectual* privacy (Koops et al., 2016). Communicational privacy of mediated and unmediated communication can be infringed when users interact with and around household IPA devices. Moreover, intellectual privacy can be at stake when IPAs influence how users develop opinions and beliefs. Finally, household IPA use can infringe spatial privacy of the private sphere and intimate activities.

In order to consider physical and virtual spaces, *territorial* privacy forms a relevant addition for this research. Territorial privacy addresses privacy around what can be observed (i.e. recorded/collected) about a person in their personal space and what can be observed by entities having virtual access to the personal space (Könings et al., 2010). This applies to household IPA use because devices are able to record audio (and some devices also video) in the physical personal space. Platform actors, third party service providers, and in some cases malicious actors, can access these recordings virtually. The following sections zoom in on how information, spatial, territorial, intellectual, and communicational privacy concerns are linked to particular surveillance, security, and platform issues.

Surveillance concerns

The increase of household IPA adoption is accompanied by growing concerns about communicational privacy of unmediated communication (Koops et al., 2016). In the past years, several issues prompted public debate about household IPAs *listening in* and acting without user requests. People were concerned about the story of a Google Home Mini recording and sending to Google servers 24/7 which was caused by a malfunctioning touch-button – now disabled on all Google Mini devices (Russakovskii, 2017). An Amazon Echo device not only recorded a private conversation, but also sent this to a random contact (Horcher, 2018). People were also made uncomfortable by reports of Amazon Echo devices laughing randomly without being prompted (Chang & Mogg, 2018). While these issues seemingly focus on isolated technical incidents, researchers found that users are often concerned about devices acting as surveillance machines. Household IPA users in the UK voiced concerns about the device listening to them constantly and were afraid that it would record intimate conversations (Manikonda et al., 2017). In addition, American non-users expressed that they felt uncomfortable with putting a device with a microphone in their private home because this would harm its sanctity (Lau et al., 2018).

Security concerns

The security of household IPAs is tested and challenged by researchers who found that there are different security vulnerabilities which can be exploited by hackers to access houses with smart doorbells and to make purchases via household IPAs (Lei et al., 2017). Because this concerns the private space in physical and virtual form, these practices infringe users’ spatial (Koops et al., 2016) as well as territorial privacy (Könings et al., 2010). Remarkably, users might increase security risks when they fail to protect their routers and connect their device to appliances with weak security (Furey & Blue, 2018).

According to Manikonda et al.’s (2017) US-based survey results, many household IPA users are concerned that their device will be hacked, they fear that this makes them vulnerable to malware or cybersecurity breaches. When users in the US were presented with three different household IPA security technologies to explore privacy and security concerns, they proved to be aware of different types of threats (such as software bugs causing erroneously behaviour and platforms/third parties listening in). Yet, they were not concerned about these threats having personal privacy implications (Chandrasekaran et al., 2018). Notably, non-users in the US displayed more concerns about household IPAs being hacked than active users (Lau et al., 2018). In general, many users are unaware of security risks and how to secure their devices (Furey & Blue, 2018).

Platform concerns

Household IPAs collect, process, and share personal data to function. Connected media accounts, smart appliances, and credit cards enable users to control entertainment services, manage smart appliances, and make purchases via their household IPAs. These practices are embedded in smart home ecosystems connected to third-party providers of services, skills, and smart appliances, something that many household IPA users are not aware of (Abdi et al., 2019). The fact that these third parties also have access to the (meta)data of IPA users complicates privacy protection and awareness, and infringes information privacy (Koops et al., 2016). Moreover, cases have been reported where governments requested household IPA recordings for law enforcing purposes (Fussel, 2020). Malkin et al. (2019) found that many American household IPA users seem to be unaware of the fact that their requests toward the device are stored. Once made aware of this, most users wanted to be able to delete recordings in order to avoid private conversations ending up in the hands of the platform owners, prevent platforms from building detailed profiles, and protect children and guests from being monitored. Huang et al. (2020) suggest that some American users are concerned about data collection by IPA platforms and about a lack of clarity and transparency around how data are used and shared.

Data collection via platforms seems to instigate the most pressing privacy concerns. For UK users, concerns about third-party developers of software/skills/apps and contractors, and to a lesser extent household IPA platforms and law enforcement are more pressing than concerns about social privacy issues (Lutz & Newlands, 2021). Interestingly, German users expressed fear that governments can request access to their household IPA data while they were less concerned about data use by IPA platforms (Pridmore & Mols, 2020). Contextual differences also become visible in how users regard different types of data. Namely, financial transactions and credit card account information are deemed more sensitive than other types of information (Huang et al., 2020; Manikonda et al., 2017; Pridmore et al., 2019).

In order to provide insight into the drivers of privacy concerns in these three different contexts, our survey follows the first exploratory research question: **Which factors influence household IPA privacy concerns in the context of surveillance, security, and platforms?**

IPA affordances

A recurring theme in discourses about household IPAs, something that also came up in our focus groups, is the notion that household IPAs enable users to *do* everyday practices differently. To makes sense of how potential users regard these activities and experiences offered by household IPAs we turn to the concept of affordances. Gibson coined the term *affordances* in 1979 to describe how environments and objects have basic properties which *afford* humans to engage in particular actions or behaviour. For instance, some objects afford to be lifted and carried (e.g., due to their shape or because they have a handle), while others do not (Gibson, 2014). Affordances can broadly be defined as *possibilities for action* which take place in relations between humans, technologies and their material features, and the situated nature of use (Evans et al., 2017).

Affordances are enacted social, physical, and technological contexts, and therefore the situational context must be considered in order to understand an object's affordances (Humphreys et al., 2018). The concept of affordances has been widely used yet there is no consistent application. Bucher and Helmond (2017) and Evans et al. (2017) present helpful analyses of different (mis)uses of the term and offer tools to analyse affordances in social media contexts. In our analysis, we build on Nagy and Neff's (2015) concept of *imagined affordances*. The concept imagined affordances includes material, mediated and emotional aspects of human-technology interaction and takes relations between designers, users, and algorithms, as well as user perceptions, emotions, and experiences into account. Imagined affordances *"emerge between users' perceptions, attitudes, and expectations; between the materiality and functionality of technologies; and between the intentions and perceptions of designers*" (Nagy & Neff, 2015, p. 5). The authors provide an example of an imagined affordance by describing how the Facebook News Feed is perceived by users as offering objective reporting of posts of their Facebook friends, *"rather than an algorithmically encoded parsing of them"* (Nagy & Neff, 2015, p. 5). This conceptualization of socio-technical imagined affordances provides useful tools to analyse mediated uses of technologies embedded in intangible platforms and operated via hidden algorithms – such as household IPAs.

Previous studies indicate that the particular affordances of household IPAs enable users to engage in specific practices. Building on affordances from a relational perspective (Evans et al., 2017), Lutz and Newlands (2021) mention how the relation between household IPAs and users brings possibilities for action in enabling interactivity, searchability, and recordability. There are no details provided about these affordances, however the authors indicate that they can enable lateral surveillance practices between family members (Lutz & Newlands, 2021). Furthermore, Brause and Blank (2020) identify three spatial affordances in household IPA use. The first is potential ubiquity, users can connect household IPAs to other devices and their phones to create seamless experiences in their IPA use. Second, household IPAs can connect spatially separated people via their link-ability. The third spatial affordance concerns control-ability which allows users to control a plethora of connected devices via one device. Finally, Cho (2019) presents voice interaction as a key affordance of IPAs. Communication via voice interaction can afford the experience of engaging in a social conversation, in contrast to less *social* experiences of text interactions. However, this effect only occurred for users with low privacy concerns, and for interactions about non-sensitive health topics (compared to more sensitive health topics) (Cho, 2019).

In the analysis of our focus groups, we aim to provide an in-depth understanding of how specific socio-technical affordances are paramount to multidimensional privacy concerns around surveillance, security, and platforms. This analysis is guided by RQ2: **What role do affordances play in household IPA privacy concerns in the context of surveillance, security, and platforms?**

Research method: Survey and focus groups

Our research design combines an exploratory survey with semi-structured focus groups in order to provide an in-depth and multidimensional understanding of household IPA privacy concerns. This study is conducted among Dutch university personnel (research as well as support staff).

Survey sampling, measurements and variables[9]

In April 2018, we distributed our survey (see Appendix 7) via email to 3000 employees of a university in the Netherlands, including university staff and research personnel. A total of 325 respondents participated in the survey, among which, 291 completed the questionnaire, resulting in a response rate of 10%. The following control variables are included:

[9] The survey analysis is led by co-author Yijing Wang.

Gender; approximately 36.2% of the final sample identified as male *(N = 114*) and 58.4% identified as female *(N = 170)* (5,4% of the respondents preferred not to answer this question). *Education level*; the majority of the participants *(55%, N = 160)* obtained a master's degree. The *age* of the respondents varied from 22 to 64 *(M=37, SD=11*). *Annual household income*; 22.7% *(N=66)* respondents indicated an income between €25k-40k, 11.3% *(N=33)* indicated €40k-50k, 17.2% *(N=50)* indicated €50k-65k, 14.4% *(N=42)* indicated €65k-85k, 14.4% *(N=42)* indicated €85k-130k, and 4.1% *(N=12)* above €130k (11,3% of the respondents preferred not to answer this question).

The majority of the respondents use either an iPhone *(N=140, 48.1%)* or an Android device *(N=136, 46.7%),* the remaining 5,2% of the respondents use a different operating system. Further, 17.9% *(N=52)* respondents indicated that they are currently using a phone IPA, whereas only 4.5% *(N=13)* respondents are using a household IPA. Household and mobile IPA use takes place in broader repertoires of everyday technology use, and IPAs are by nature interconnected with smartphones, entertainment services, and other technologies. Therefore, our survey explores privacy perceptions around household IPAs in the broader context of everyday technology use. We aimed to identify how IPA-focused privacy concerns relate to more general perceptions around Internet familiarity, digital literacy, general privacy concerns, mobile privacy concerns, mobile privacy confidence, and smartphone reliance. Below follow descriptions of the dependent and independent variables. The full survey is included in Appendix 7 and an overview of the reliability tests is presented in Table 3.

Dependent variables (all developed for this survey)

Household IPA surveillance concerns

This variable measures how concerned respondents are about IPA devices functioning as a surveilling agent. Two items are combined into one variable through a weighted averaged method. The first item is *"I am concerned that the device is always listening,"* and the second item is *"I am concerned that the device is always recording any sounds in the room".* Both statements were followed by a 5-point scale from *"Not at all concerned"* to *"Extremely* *concerned".* The reliability test shows a modest internal consistence of the items *(α = .681, M = 2.739, SD = 1.043)*.

Household IPA security concerns

This variable measures how concerned respondents are about security vulnerabilities of household IPAs being exploited. Two items are combined into one variable through a weighted averaged method, which are *"I am concerned that other people might activate/access the device and trigger unauthorised purchases,"* and *"I am concerned that other people might activate/access the device and disrupt my Internet accounts or personal information".* The reliability test shows a good internal consistence of the items *(α = .720, M = 3.371, SD = 1.111)*.

Household IPA platform concerns

This variable measures concern about household IPA data being stored and used by law enforcement, third parties, and platforms. Three items are combined into one variable through a weighted average method. An example is *"I am concerned that my questions directed at the device are stored and sold to third parties (e.g., advertisers)".* The reliability test shows a high internal consistence of the items *(α = .849, M = 3.538, SD = 1.088)*. Table 4 shows the correlation matrix of the constructed variables. Among the three dependent variables, we observe a positive correlation between *Household IPA surveillance concern* and *Household IPA security concern (r = .695, p < .01)*, and between *Household IPA surveillance concern* and *Household IPA platform concern (r = .596, p < .01)*. The strongest correlation is found between *Household IPA security concern* and *Household IPA platform concern (r = .810, p < .01)*.

Independent variables

Internet familiarity

This variable uses Hargittai and Hsieh's (2012) 10-item Abbreviated Web-Use Skills Index for the General Population. This scale is often used as a variable in surveys regarding privacy decisions (Fiesler et al., 2017; Zimmer et al., 2020). The reliability test shows a high internal consistence of the items *(α = .883, M = 4.023, SD = 0.76)*.

Digital literacy (related to smartphone use)

Developed for this survey, this 20-item variable measures respondents' level of confidence with regard to conducting particular tasks on their smartphones. The reliability test shows a high internal consistence of the items *(α = .902, M = 4.105, SD = 0.804)*.

General Privacy Concerns

We used Vitak's 12-item general privacy concerns scale (2015), this scale is also used by Vitak and others in different contexts, such as fitness trackers and social media use (Vitak, 2016; Vitak et al., 2018) and Facebook use among colleagues (Van Prooijen et al., 2018). This variable maps how concerned respondents are about risks related to digital communication technologies via a 5-point scale from *"Not at all concerned"* to *"Extremely concerned"*.. The reliability test shows a high internal consistence of the items *(α = .918, M = 3.183, SD = 0.901)*.

Mobile privacy concerns

This variable uses Xu et al.'s 9-item mobile users' information privacy concerns scale (2012) including questions about perceived surveillance, perceived intrusion, and secondary use of personal information. This scale is also used in research about health apps (Bol, Helberger, et al., 2018). A high internal consistency of the items is observed *(α = .920, M = 3.965, SD = 0.737)*.

Mobile privacy confidence

Mobile privacy confidence is measured by four items, designed for this chapter, which measure how confident respondents feel about their mobile privacy. The internal consistency of the constructed variable is modest but acceptable *(α = .644, M = 2.169, SD = 0.736)*. While the alpha is close to the 0.7 threshold, it still indicates a good reliability of the measurement.

Household IPA familiarity

Household IPA familiarity (constructed for this chapter) is measured as a 0/1 variable based on respondents' familiarity with either *"Google Home / Home Mini," "Amazon Echo / Echo Dot,"* or *"Apple HomePod"* (value=1), or none of those (value=0).

Phone IPA use

This variable is designed for this chapter and constructed from the question *"Do you have Siri, Google Assistant, or another intelligent personal assistant (IPA) activities on your smartphone?"* Respondents who answered *"Yes, I currently use it"* are assigned to one group (value=1), whereas the rest who chose another answer (*"My phone has this feature but I've never used it," "No, and I have disabled this feature," or "No, there isn't a service like that available on my phone"*) are assigned to the other group (value=0). Hence, a 0/1 dummy variable is created.

Smartphone reliance

This variable (constructed for this chapter) is measured by two items on a 100-point slider scale. Respondents indicate how often they access their smartphone and how anxious they feel after leaving the house without their smartphone. Both items reflect a respondent's smartphone reliance, and thus are combined to construct the variable. The internal consistency of the constructed variable is modest but acceptable *(α = .635, M = 61.085, SD = 21.569).*

Table 3. Descriptive statistics and internal consistency of variables

Variable	Mean	Std. Dev.	Cronbach’s α
Internet familiarity (IF) (10 items, 5-point scale)	4.023	0.76	.883
Digital literacy (DL) (10 items, 5-point scale)	4.105	0.804	.902
General privacy concerns (GPC) (12 items, 5-point scale)	3.183	0.901	.918
Mobile privacy concerns (MC) (9 items, 5-point scale)	3.965	0.737	.920
Mobile privacy confidence (MCF) (4 items, 5-point scale)	2.169	0.736	.644
Household IPA surveillance concerns (HSU) (2 items, 5-point scale)	2.739	1.043	.681*
Household IPA security concerns (HSE) (2 items, 5-point scale)	3.371	1.111	.720*
Household IPA platform concerns (HPA) (3 items, 5-point scale)	3.538	1.088	.849
Smartphone reliance (SR) (2 items, 0-100)	61.085	21.569	.644*

1) *Spearman-Brown coefficients are reported for variables measured through 2-item scales
2) N=291

Table 4. Correlation matrix

	IF	DL	GPC	MC	MCF	HSU	HSE	HPA	SR
IF	1								
DL	.450**	1							
GPC	.033	.028	1						
MC	.028	-.060	.454**	1					
MCF	.149*	.294**	-.155*	-.365**	1				
HSU	.007	-.066	.456**	.430**	-.195**	1			
HSE	.073	-.030	.443**	.511**	-.246**	.695**	1		
HPA	.098	-.071	.409**	.598**	-.269**	.596**	.810**	1	
SR	.155*	.223**	.084	-.055	-.004	.048	.063	-.008	1

1) ** p < 0.01. * p < 0.05. 2) N=291

Focus group design and analysis

We used an experimental focus group design aimed at collecting rich data. Details about the sampling, focus groups procedure, and analysis are detailed in Chapter 2. Appendix 3 includes a respondent overview of the focus groups and Appendix 7 provides the focus group guide. The codes resulting from the three phase constructivist grounded theory process are visible in the codebook in Appendix 14 (Charmaz, 2014; Corbin & Strauss, 1990). The results section presents translated quotes of the focus groups and connects these to existing research and particular affordances to provide an in-depth account of the three different household IPA privacy concerns. To contextualise the results, a note needs to be made regarding the familiarity with household IPAs. Only two participants (Hannah and Mark) owned a household IPA at the time the focus groups took place (May 2018). Because smart speakers were not officially available on the Dutch Market, they could only operate these in English and could not connect them to many services. Moreover, four respondents (Bjorn, Julia, Anna, Linda) experienced the use of smart speakers when they visited friends in the UK and US.

Results: Surveillance, security, and platform concerns

Survey results: Factors influencing surveillance, security, and platform concerns

To assess the factors influencing different household IPA privacy concerns around surveillance, security, and platforms (RQ1), we conducted three ordinary least squares regression analyses. Their results are summarised in Table 5.

Model 1 shows the impact of constructed independent variables on household IPA *surveillance* concerns. The results reveal that if general privacy concerns are perceived higher, it will lead to a higher household IPA surveillance concern (β = .405, SE = .077, p < .001). Also, higher mobile privacy concerns correspond to higher household IPA surveillance concerns (β = .403, SE = .099, p <.001). Interestingly, a significant difference is detected between people who currently use a phone IPA versus others who do not. Phone IPA users are found to be concerned less about household IPA surveillance than non-users (β = -.348, SE = .175, p < .05). One potential explanation is that the experience of using a phone IPA helps people lower their concerns about household IPAs *listening in* or recording conversations because they have overcome or have never experienced such concerns toward their phone IPA. Another potential explanation could be an unidentified common factor, which drives peoples’ intention to use IPAs, both on phones and at home.

Model 2 in Table 5 shows the impact of constructed independent variables on household IPA *security* concerns. The results reveal a positive relationship between general privacy concerns and household IPA security concern (β = .262, SE = .078, p < .001), as well as a positive relationship between mobile privacy concerns and household IPA security concern (β = .589, SE = .100, p < .001). Phone IPA users are found to be concerned less about household IPA security issues than non-users (β = -.460, SE = .177, p < .01).

In addition, different from the results of Model 1, we found a positive impact of household IPA familiarity on household IPA security concern (β = .198, SE = .059, p < .001). It implies that people with knowledge of household IPAs are more concerned about its security risks, compared to those who know less about such devices. It might be the case that these people have heard about household IPAs via newspaper articles about the devices laughing unexpectedly which were covered in Dutch news media a couple of weeks before our survey was conducted (‘Creepy’, 2018).

Model 3 in Table 5 shows the impact of constructed independent variables on household IPA *platform* concerns. The results reveal a positive relationship between general privacy concerns and household IPA platform concerns (β = .157, SE = .074, p < .05), and a positive relationship between mobile privacy concern and household IPA security concern (β = .695, SE = .095, p < .001). Phone IPA users are found to be less concerned about household IPA platforms than non-users (β = -.442, SE = .168, p < .01).

And similar to Model 2, we found a positive impact of household IPA familiarity on household IPA platform concerns (β = .159, SE = .056, p < .01). In addition, a comparison of the R-square (see Table 5) shows the difference in explained variance between the three models: The independent variables were most predictive and accounted for most variance in Model 3 (platform concerns), followed by Model 2 (security concerns) and Model 1 (surveillance concerns).

The most striking finding is the fact that respondents who are familiar with household IPAs are found to be more concerned when it comes to household IPA security and platform concerns than they are about surveillance aspects. This might suggest that being exposed to information about household IPAs (via commercials, through experiences of peers, or by having interacted with a device) lowers *creepy* associations of devices functioning as surveillance agents.

In contrast, this familiarity sparks concerns about platform data collection, processing, and sharing, and household IPA security. This finding emphasises the need for more diversified approaches towards household IPA concerns (Lutz & Newlands, 2021; Manikonda et al., 2017), as it confirms that these are not uniform.

Table 5. Household IPA *surveillance*, *security,* and *platform* concerns

	Model 1	**Model 2**	**Model 3**
	DV = Household IPA *surveillance* concerns	**DV = Household IPA *security* concerns**	**DV = Household IPA *platform* concerns**
	Parameter Estimates: Beta (S.E.)		
Internet familiarity	-.026 (.100)	.018 (.101)	.156 (.096)
Smartphone reliance	-.001 (.003)	.001 (.003)	-.001 (.003)
Digital literacy	-.029 (.091)	-.034 (.092)	-.136 (.087)
General privacy concerns	.405 (.077)***	.262 (.078)***	.157 (.074)*
Mobile privacy concerns	.403 (.099)***	.589 (.100)***	.695 (.095)***
Mobile privacy confidence	-.082 (.091)	-.110 (.092)	-.060 (.087)
Phone IPA use (Yes)	-.348 (.175)*	-.460 (.177)**	-.442 (.168)**
Household IPA familiarity	.094 (.058)	.198 (.059)***	.159 (.056)**
Gender	.134 (.092)	.138 (.093)	.165 (.088)
Age	.002 (.006)	-.002 (.006)	.001 (.006)
Education	-.033 (.056)	-.039 (.057)	.037 (.054)
Household	.008 (.060)	-.033 (.061)	.019 (.057)
Income	.031 (.037)	.039 (.037)	-.021 (.035)
Constant	.001 (.769)	.264 (.778)	-.187 (.738)
F-value	7.552 p<0.001	8.672 p<0.001	10.327 p<0.001
R-square	.321	.351	.393

1) *** p < 0.001. ** p < 0.01. * p < 0.05.   2) N=291.

Focus group results: Surveillance, security and platform concerns

The focus group conversations highlight how household IPA concerns are embedded in broader repertoires of everyday technology use:

> *“I have a smartphone, and I’m very keen on protecting my privacy. My location tracking is always disabled, I switched off Wi-Fi completely, so that I cannot be followed, I’m very keen on that, and that’s why I like to think about things like this…I tried to use Siri on the iPad, but it didn’t feel comfortable to me…And no, I don’t see myself using this [household IPA], I’m not very enthusiastic.”* (Jay, communication)

Jay’s quote shows how he wants to control the collection and access to his personal information, protecting his information privacy underpins his technology use. Supporting the survey results, Jay’s general privacy concerns and concerns around mobile privacy led to higher privacy concerns about household IPA use. His quote indicates that he does not want to be followed or tracked, yet the data collection and recording features of household IPAs afford platforms *searchability* and *recordability* (Lutz & Newlands, 2021). These affordances motivate Jay to refrain from using IPAs. In answer to RQ2, the focus groups indicate that other affordances also play a role in particular household IPA privacy concerns in the context of surveillance, security, and platforms.

Surveillance concerns around conversation and recordability affordances

Household IPAs can be controlled via voice-activation. This feature affords conversations with the devices. During the focus groups, the respondents tried out a Google Home and interacted with the device. Many of our respondents find this *conversation* affordance uncomfortable. Leah (organization support) states: *“If it can respond and you can have a conversation, I would find that scary…I see myself alone in my apartment talking to a device, yeah, I don’t know, I find that weird”.* Mona reflects on her family context: *“I would not like to have this interaction in my family…I just don’t feel comfortable with saying a command and ask it to do something, it is just a thing”.* While these experiences from potential household IPA users might be influenced by the novelty of this experience, these findings resonate with American non-users who also feel uncomfortable about this conversation affordance (Lau et al., 2018).

These uncomfortable feelings are interconnected with another affordance, namely *recordability* (also described by Lutz and Newlands, 2021). For a household IPA to afford conversation, the device needs to record user requests which activate IPA responses or actions. It became clear that our respondents vary in their attitudes towards recordability, many do not trust the device to only listen when the trigger word is used. They are concerned that the devices are constantly *listening in* and recording conversations and environmental sounds, a finding that resonates with earlier research (Manikonda et al., 2017). These concerns were discussed in focus group 1:

> Jessica (Marketing): *"Companies like Google and Apple will definitely save everything you say to Siri or whoever, and not particularly to listen to each specific word, but to use all your commands to create a whole, a sort of, image of who you are and what your interests are. I find that very scary, and with something like this [household IPA], this only gets worse."*
> Interviewer: *"Mm-hm, and are there particular things you deliberately don't want to share with such a device?"*
> Kim (PhD candidate): *"Well, it is more that you suddenly have to pay attention to what you say. Because, yeah, you never know who's listening…And then that raises the question: 'Okay, I'm now having a private conversation, or whatever, and eh, do I want others to hear that?' No, of course not!"*

Whereas Kim feels that private conversations should not be recorded by household IPAs, Marcus (IT) does not deem living room conversations sensitive: *"What would be hackable of these devices? Only that someone can listen in from a distance in your living room. I dare to state that most living room conversations are not interesting at all".* Respondents clearly have different perceptions of the sensitivity of personal conversations in the intimate sphere of the home. Respondents also have different perceptions of the consequences of the recordability affordance. Some respondents share pragmatic attitudes towards technology. For instance, Charlie (professor) beliefs that it is impossible to listen in on *“all these Siri devices”,* because this would require too much data processing and manpower. Charlie perceives recordability as an affordance in a less concerned manner than most respondents because he deems it impossible that household IPAs are continuously recording. His perceptions resonate with previous research wherein American users stated that it would be impossible for companies to store and process all the data of continuously recording devices (Lau et al., 2018).

Household IPA use and its conversation and recordability affordances produces different concerns around communication privacy. Some regard the content of mediated interactions with the device and unmediated interactions around the device sensitive, while others are more pragmatic and do not perceive these as sensitive or deem it unlikely that all conversations and interactions can be recorded and processed. This shows that the situatedness of technology use determines how particular affordances are perceived (Evans et al., 2017; Humphreys et al., 2018).

Household IPA security concerns around locatability affordance

When it comes to concerns around household IPA security, prior research indicates that users and non-users are mainly concerned about the devices being hacked which leads to malware or cybersecurity breaches (Manikonda et al., 2017). In contrast, our respondents are more concerned about break-ins into their house. Unexpectedly, these concerns about break-ins came up in three out of six focus group discussions. For example, Peggy (education support) brought this up when the conversation addressed drawbacks of household IPA use: *“If someone would hack this, they could easily see when you’re not at home, when there are no activities, and when you look at break-ins, I’m curious how people can deal with that”.* In another focus group discussion, Bjorn (PhD candidate) shared similar concerns: *“There will be a moment when these devices will be hacked. Without a doubt. And when that information comes out, you have, well then you can easily map when someone’s home and away. So that is very interesting information for burglars”.* Furthermore, Linda (professor) shares that she does not feel comfortable with booking a hotel via a household IPA. She is afraid to share information with the device about when she plans to be away, and that this in turn allows others to ask the device *"Hey Google, when will she return?"* Linda is not concerned about her data being stolen; she is afraid that burglars will consult the device to find out when she is away. While existing research approaches security in the context of information privacy (Chandrasekaran et al., 2018; Furey & Blue, 2018; Lei et al., 2017; Manikonda et al., 2017), our respondents share concerns about their spatial and territorial privacy of their private space and intimate activities (Könings et al., 2010; Koops et al., 2016).

This is caused by how they perceive their devices to be connected to their homes and their personal space. The *locatability* affordance could enable hackers to locate users (and use patterns) within their intimate sphere. Moreover, respondents fear that hackers can infringe their spatial and territorial privacy by taking over their devices. Mark (education support) shares his fears: *"They [hackers] can listen to your voice, but can also hear what happens in your home,"* to which Hannah (education support) adds: *"And switch on your microphone".* These concerns further highlight how our respondents' privacy concerns in the context of security boil down to tangible threats that directly impact their intimate home contexts.

Platform concerns around control-ability and assistance affordances

The final type of household IPA privacy concerns is characterised as more intangible because it regards data collection by platforms. As Babette (researcher/lecturer) describes: *"I am concerned about privacy and everything that is stored of the things you do".* Robert (IT department) voices similar concerns "*I am critical towards new technologies when it comes to privacy, I am pretty concerned about what they all collect".* More specifically, respondents are critical towards the use of the data that is stored about their activities and their conversations. Household IPAs collect data to afford *control-ability* (coined by Brause and Blank, 2020), they allow users to control other appliances, devices, and accounts via their household IPA. This technical affordance is embedded in platform ecosystems wherein user data are shared with third-party providers of smart appliances, services, and skills (Abdi et al., 2019). Echoing prior research (Huang et al., 2020; Malkin et al., 2019), our respondents indicate that their concerns are fuelled by platforms' lack of transparency around data collection, processing, and sharing. For instance, Dennis states:

> *"I'm really a privacy-watcher. And, before I investigated it, I will not activate a functionality…Maybe when I've looked into it, I'll know what type of data or information is being stored. But for me it's: If I've not looked into it, I will not use it. And for functionalities like these [household IPAs], it is hard to find out what exactly they do with [personal data]. Or how much you give away and how much control you have."* (Dennis, IT department)

The affordance control-ability complicates data collection, processing, and sharing in an opaque manner. For many (potential) users, it remains unclear what data are shared with what other parties and what these parties in turn do with their data. This makes it difficult for users to protect their information privacy (Koops et al., 2016), and for some respondents like Dennis, a lack of transparency forms the reason for not using IPAs. Ironically, the affordance control-ability allows users to control their smart homes, yet it prevents them from controlling their information privacy.

A key concern that emerged from multiple focus groups is related the affordance of *assistance*. Household IPA platform ecosystems afford users to activate a plethora of services to assist them. For example, they can provide data about their daily commute so that the device can suggest taking another route when there is a traffic jam. Or they can provide access to their email accounts and streaming services to receive notifications of new entertainment releases and flight changes for purchased tickets. Some respondents were afraid that their own actions and decisions will be affected by a household IPA that constantly assists them. Karen (professor) fears that she will become too dependent on the device: *"You become dependent, I think, that concerns me, yes, that when you put this [household IPA] in your house, that you will not think about what is in agenda for tomorrow, but that you'll ask that thing".* Similarly, Monica (communication) fears that she will rely too much on the device: *"You know how your grammar might be degrading more because text prediction? I thought the same, with all these services that I would not want to become so reliant on it that I wouldn't know what to do if it disappeared from my life".*

For these respondents, the assistance affordance can harm their intellectual privacy by influencing their decisions and routines (Koops et al., 2016). The fact that the risks that they foresee are related to their own behaviour adds insights to privacy decisions specific for the use of household IPAs. Bjorn (PhD candidate) is particularly concerned that selections in notifications and information might be used to influence behaviour: *“I believe that you’re unknowingly, or maybe even knowingly, part of a huge Google A/B test”.* Bjorn fears that data collection for assistance leads to the device not only influencing his behaviour but also testing how he reacts to the suggestions and adapt these accordingly. This mirrors general concerns about how the embeddedness of voice-activated assistants in everyday life have the potential to change behaviour and actions. In combination with the earlier mentioned recordability affordance, assistance can have a chilling effect by affecting how users behave in their private space. Karen, Monica, and Bjorn display awareness of data collection and about potential influences on their behaviour. When such awareness makes them adopt particular behaviour to avoid undesired actions being recorded by the device a chilling effect occurs (a practice also described by Büchi et al., 2020 in relation to algorithmic profiling). Moreover, existing research emphasises the expectation that household IPA use can ultimately affect how our memory works (Atkinson & Barker, 2020).

Conclusion: Pragmatic multidimensional privacy concerns

This mixed-methods chapter presents an in-depth and differentiated account of privacy concerns around household IPAs. We provide insights about a continental European population on the cusp of normalizing such devices in the home. This sample is culturally distinctive from most other studies, and in this discussion, we provide insights in how Dutch respondents differ from populations studied in existing research (mainly US and UK oriented). We also reflect on the implications of our findings, in particular on how affordances amplify privacy concerns.

Our survey results show overlap in the factors influencing surveillance, security, and platform concerns, yet they also show where these concerns differentiate. First, the finding that general privacy and mobile privacy concerns lead to higher household IPA surveillance concerns across the board indicates that existing privacy concerns extend to novel technologies and potentially amplify them. In contrast, phone IPA use lowered all three types of concerns, which indicates that privacy considerations already resulted in phone IPA use and that using similar technologies might lower the threshold to household IPA adoption. However, surprisingly the survey results indicate that whereas IPA familiarity correlates with more concerns around security and platforms, this is not the case for concerns about surveillance itself. This suggests that familiarization lowers the more concerning or creepy associations of devices listening in as surveillance agents, but simultaneously sparks concerns about platforms and household IPA security. While the first two findings simply illustrate a trajectory – of already existing concerns (privacy) and acceptance of already existing devices (phone IPA use) increasing in relation to these devices – the last finding shows a more nuanced view. **Platforms themselves are seen as a more important factor than the surveillance they may afford as is the security of the device more concerning than the surveillance it may afford**.

The focus groups provide insights into the perceptions and experiences behind diversified privacy concerns and indicate how these are tied to particular affordances. Interestingly, **most respondents focus more on immediate and physical risks and have a pragmatic perspective towards hypothetical and long-lasting risks**. With regards to the latter, the focus group results show overlap between our Dutch respondents and existing research. Namely, US-based research indicates that concerns about *recordability* and *listening in* are dissuaded by pragmatic attitudes based on how impossible it is for platforms to store and process recordings of all devices all the time (Lau et al., 2018). This pragmatic perception was also shared by some of our respondents. In addition, many respondents felt uncomfortable in interacting with the device (*conversation* affordance), resonating research about non-users (Lau et al., 2018). This indicates that uncomfortable feelings can also motivate consumers to refrain from using household IPAs. Four our respondents, some of these uncomfortable experiences might have to do with the novelty of household IPAs but also with the fact that it is not very common to be talking to devices in the Netherlands. Mirroring the authors' assumptions, focus group respondents shared that talking out loud to smartphones (without holding the phone to the ear) is mainly restricted to younger smartphone users and not (yet) a widespread practice.

The most striking finding of the focus groups substantiates the survey’s security concerns as these prove to be connected to the *locatability* affordance. Whereas existing research indicates that (non-) users are concerned about security and fear for information privacy (Lau et al., 2018; Manikonda et al., 2017), our respondents perceive insufficient or failing device security as a risk potentially leading to house break-ins. This is caused by household IPAs’ interconnectedness with the home context, affording locatability as it might enable hackers to determine the physical location of users and their devices. Our respondents’ concerns around device security are closely connected with spatial and territorial privacy (Könings et al., 2010; Koops et al., 2016) because these risks are perceived as threatening intimate home contexts. The physical and tangible nature of these threats seems unique for our respondents in light of existing research. This might be influenced by a more familial connection to local space in terms of expectations of openness (such as illustrated in social norms around open curtains in the Netherlands, see Horst and Messing, 2006). This openness goes hand in hand with social control and the active safeguarding of neighbourhoods (as discussed in Chapters 3 and 4). **Being more aware of physical safety concerns might cause people in the Netherlands to perceive more tangible risks around household IPA devices.**

Moreover, affordances in relation to platform concerns also reveal similarities and differences with existing research. The affordance *control-ability* (Brause and Blank, 2020) instigates concerns about a lack of transparency around data collection, processing and sharing, resonating research among US and UK household IPA users (Huang et al., 2020; Malkin et al., 2019). Concerns that we have not seen to be reflected in existing research, revolve around household IPAs assistance affordance. This affordance initiates concerns around intellectual privacy (Koops et al., 2017) because respondents fear that the algorithmically driven suggestions and assistance of the device will influence their behaviour and their decisions.

Limitations and directions for future research

While our research highlights important aspects of user privacy decisions and potential uses of household IPAs, it is based on a one-time survey and focus groups. Our research sample is limited to university employees and its results may not be generalizable to a wider Dutch population. University employees might have higher privacy concerns and awareness compared to a representative sample of Dutch citizens. While we aimed to increase the diversity in our sample by including both support staff and academic employees, future research should focus on a more representative sample. Furthermore, our sample of potential users (and a few early adopters) did not allow for an exploration of privacy concerns around shared use and other household members, an aspect of household IPA use that can lead to power imbalance (e.g., see Geeng & Roesner, 2019; Huang et al., 2020; Lutz & Newlands, 2021).

Following Lutz and Newlands (2021) and Manikonda et al. (2017), our findings emphasise the need for more diversified approaches towards household IPA privacy concerns. They confirm that privacy concerns are not uniform but concern information, communicational, intellectual, spatial, and territorial privacy (Könings et al., 2010; Koops et al., 2016). Future explorations of the multidimensionality of privacy concerns around household IPAs or other smart home devices and services will bring insights into which aspects matter most to (potential) users. These insights can not only inform privacy awareness raising initiatives but can also indicate where gaps in privacy literacy reside (e.g., fears about physical threats to spatial privacy may indicate limited knowledge or awareness about identity theft and data breaches). Our focus groups also show how a qualitative approach to multidimensional privacy concerns allows for unexpected findings, such as the tangible nature of IPA security concerns we found. Therefore, more qualitative approaches to privacy concerns around IPAs and other technologies will provide more context and insights into motivations behind privacy attitudes.

Chapter 8

“Friends’ parents are probably a lot less strict” Family surveillance in interconnected families[10]

Introduction

Nowadays, most adolescents grow up in interconnected family homes saturated with technologies and they have access to social media and messaging apps. In contrast, their parents came of age in a time when personal computers and mobile phones were first being introduced. Due to the omnipresence of digital technologies, parents nowadays have a plethora of parental monitoring tools at their disposal. These range from dedicated technologies like parental control tools and location tracking apps to more elementary solutions such as befriending their children on social media or accessing smartphones (Marsh et al., 2017; Marx & Steeves, 2010). This paints a stark contrast with the past, where such technologies were not available. Parental monitoring practices have evolved over the years and form an indication of the changing sociomaterial nature of parenthood. The current abundance of parental monitoring opportunities poses a challenge for parents who have to balance safeguarding their children against providing them with freedom to develop themselves. This chapter explores the monitoring practices of Dutch parents that have not experienced digital parental monitoring during their own youth.

As indicated in the introductory chapter, surveillance is embedded in everyday life (Lyon, 2018). Researchers emphasise that parental monitoring practices concern a form of surveillance that goes hand in hand with normative assumptions about good parenting, safety, and risky behaviour (Leaver, 2015; Rooney, 2010; Simpson, 2014; Steeves, 2014). Parental monitoring entails considerations of control, freedom, privacy, and care. As such, monitoring practices can lead to tensions and can

[10] Chapter under review for *ACM Conference on Human Factors in Computing Systems (CHI) 2022.*

restrain children and (early) adolescents in maintaining privacy, having autonomy, and developing independence (Bennett et al., 2014; Nelson & Garey, 2009; Simpson, 2014). However, while many digital monitoring tools are available, research shows that many parents control their children's technology use via low-tech solutions and rules (Brisson-Boivin, 2018; Livingstone & Blum-Ross, 2020; Mazmanian & Lanette, 2017; Vasalou et al., 2012; Zepan & Črnič, 2018).

To broaden the scope of parental monitoring more explicitly to surveillance practices, family surveillance is investigated as **practices to keep track of children's digital and non-digital activities and associations.** I explore how families experience surveillance practices and build on interviews with parents and children in order to answer the research questions: 1) **How do Dutch parents and early adolescents experience family surveillance?** and 2) **How do Dutch parents engage in (non) digital parental monitoring practices?** It is important to note that (non)digital could also have been described as online/offline. However, this distinction is untenable in interconnected families where online and offline activities take place simultaneously and boundaries between digital and physical contexts often and easily collapse (Pagh, 2020).

This research focuses on nine Dutch families with at least one child in the phase of early adolescence. Privacy scholars advocate to increase the role of children in privacy and media research because their perspective is often neglected (De Leyn et al., 2021; Mazmanian & Lanette, 2017; Steeves et al., 2020; Stoilova et al., 2019; Wolf & Abeele, 2020; Zepan & Črnič, 2018). Therefore, I interviewed eleven early adolescents and eleven parents. The phase of early adolescence can roughly be categorised as 10-16 year old (Steinberg & Silverberg, 1986). This is a phase wherein children become more emotionally autonomous in relation to their parents as they *"relinquish some of their childish dependencies on them, and form a more individuated sense of self"* (Steinberg & Silverberg, 1986, p. 848). In the Dutch context, this is also the moment when children transition from primary to secondary school, an impactful transition from a small-scale school to a much larger secondary school (Van Rens et al., 2019). Logistically, this often entails a change from walking or biking to a primary school located within or nearby their neighbourhood to biking to a secondary school that is located further from their home. Moreover, this research took place during the Covid-19 pandemic, when restrictions led to the family home becoming the place where work, online education, digital social connections, and other activities intertwined. This provides a unique view on family dynamics around technology.

The results section shows that family surveillance in Dutch families is established on a basis of open communication. Some parents are motivated to use digital monitoring tools to safeguard and guide their children, while others refrain from surveillance practices to prioritise freedom and trust. Before these findings are illustrated by quotes from the interviews, literature about different forms of parental monitoring and reflections on the consequences of family surveillance are presented in the next section.

Literature: Parental monitoring as family surveillance

Family surveillance practices revolve around taking care of family members while also controlling them (Nelson & Garey, 2009). Controlling children's behaviour is inextricably linked with parenting itself and monitoring is crucial for protecting children against physical harm – also in contexts where parents cannot supervise them directly (Kerr et al., 2010; Stattin & Kerr, 2000). Public debates and marketing around parental monitoring contain normative accounts of care, control, and good parenting. Parental monitoring is normalised throughout childhood and digital surveillance is equated with care and good parenting (Steeves, 2014). By not engaging in parental monitoring, parents risk to neglect their responsibility of keeping their child safe (Simpson, 2014).

According to Katz (2001), parental monitoring technologies promulgate a state of *hypervigilance* that can be characterised by households with little regard for children's privacy, self-determination, or a presumption of innocence. The latter is visible in how the marketing of location tracking apps often presents children as incompetent. They are in need of being tracked and location tracking provides freedom for an interconnected family. These suggestions are potentially dangerous because they can stand in the way of children developing agency, resilience, and self-reliance (Simpson, 2014). This section explores how technologies amplify family surveillance practices around monitoring screen time, locations, and online and offline behaviour of (early) adolescents. It also provides insights into academic reflections on the consequences of family surveillance and parental monitoring. The chapter concludes with an overview of research into the role of communication in relation to parental monitoring.

Parental monitoring practices

Parental concerns exist around their children’s activities, interactions, and influences of peers, classmates, and others (Kurz, 2009). Marketers of monitoring tools and experts highlight that online, children face risks such as encountering inappropriate or questionable content, communicating with strangers, or being target or engaging in cyberbullying (Marsh et al., 2017; Marx & Steeves, 2010). Whereas parents can monitor their children by accompanying them, organising activities within the family home, or getting adolescents involved in activities that take place in supervised environments (such as sports or other after-school activities) (Kurz, 2009), some parents rely on monitoring technologies to keep an eye of their teen’s whereabouts, activities and interactions. While very young children will not verbally resist parental monitoring, tensions around family surveillance can occur when (early) adolescents dislike the feeling of being monitored by their parents (Nelson & Garey, 2009). Discussions about media use can lead to conflicts between parents and children, for instance about excessive use of digital devices or online activities (Brisson-Boivin, 2018).

Monitoring location

For many parents, the process of enabling their children to be outside unsupervised and to travel independently entails the balancing of control and monitoring versus trust and freedom. Parents adopt different strategies to deal with such dilemmas and for some this entails the active monitoring of their child’s location. Many parents ask their children to message or call them regularly or when they to go to another location. Yet, it is not always easy to reach children on their smartphones and they can lie about their whereabouts (Ervasti et al., 2016; Kurz, 2009).

Therefore, some parents use technologies like global positioning system (GPS) devices in the form of watches or tags placed in backpacks or clothing (G. T. Marx & Steeves, 2010), or they check the GPS location of their child’s smartphone. A popular example is the smartphone application Life360 that allows for location tracking, checking in, and for alarming family members in case of danger (‘Check In & Panic’, 2012). According to Simpson (2014), Life360 not only provides peace of mind, but also enables parents to take action when children enter an area deemed unsafe or inappropriate. Parents can benefit from an increased sense of control and family safety and children might enjoy more freedom independently. Similarly, primary school location tracking tools provide peace of mind and reassurance to Finnish parents and children (Ervasti et al., 2016). Yet, location tracking can also undermine privacy rights. On the one hand because parents decide for children that they will be monitored, and on the other hand because GPS tracking results in large databases of children’s movements. Moreover, GPS tracking is said to redefine family dynamics. Overprotective parenting can deprive children of the opportunity to explore independently and can limit children in developing resilience (Simpson, 2014). Some parents in the UK find location tracking unnecessary because they feel that it harms children’s self-direction and trust. Instead, they relied on adult supervision, children’s peers, setting clear rules, and the use of smartphones to keep informed of their children’s whereabouts (Vasalou et al., 2012).

Monitoring screen time

In most family homes, a multitude of devices is available. Children use smartphones and other interconnected devices for entertainment, homework, social media, and communication purposes. Most parents fear that too much screen time is bad for their children. For example, parents in the US are concerned about their child’s brain development, erosion of interpersonal skills, reduced desire for creative play, and increased aggressive behaviour (Mazmanian & Lanette, 2017). Similarly, when choosing from a variety of rules (e.g., about privacy, access, education, gaming, data retention, and protecting children against inappropriate content), Dutch parents find screen time boundaries the most important topic (YoungWorks, 2014).

There are different ways to manage screen time. Parents can set rules, ask children to stop using their devices, shut down or take devices away, or replace devices with other activities (Marsh et al., 2017; Nikken, 2021).

There is also software available that enables parents to install time limits on Wi-Fi and to filter inappropriate content (Cino et al., 2020). Contrastingly, screen time can also be used as a reward for having completed tasks for school or in the household (Mazmanian & Lanette, 2017; Zepan & Črnič, 2018). Some parents also opt for more flexible and contextual approaches by separating the time spent from the nature and quality of digital activities (Livingstone & Blum-Ross, 2020). When it comes to (early) adolescents, experts support the use of rules to manage screen time, such as banning devices during dinner time, but stress that it is important to involve children in designing these rules (Marsh et al., 2017).

Monitoring online behaviour

Children’s online activities form a third parental challenge. Parents have no direct oversight on the online spaces their children frequent, nor on the digital interactions they engage in. They fear offensive sexual or violent online content, online harassment and cyberbullying, and inappropriate online behaviour and identities (Brisson-Boivin, 2018; Mazmanian & Lanette, 2017). These concerns can be clustered respectively as concerns around content (what children consume online), contact (with whom they engage online), and conduct (how they interact online) (Brisson-Boivin, 2018; Trinity McQueen, 2018, based on Livingstone et al., 2015). Many parents aim to limit the risks of digital media by urging their children to tell them or another parent/guardian if they experience something online that makes them uncomfortable (Brisson-Boivin, 2018). Some parents also actively control their children’s social media use (Bennett et al., 2014). In order to protect children online, parents can use elementary monitoring methods by checking social media activity and messages to monitor how children behave and interact online (Marsh et al., 2017). They can also make use of parental control software which blocks questionable content and logs online behaviour (Marsh et al., 2017; Marx & Steeves, 2010). The monitoring of online behaviour can limit adolescents in their development, because they need trust and privacy to separate themselves from their families and develop a sense of responsibility (Bennett et al., 2014). Steeves (2014) emphasises that pervasive online monitoring is problematic because (early) adolescents use technologies to learn new things, explore the world, and connect with friends. Digital monitoring can *"shut down online spaces for these uses, especially identity play and connecting with friends, because the lack of privacy made it more difficult to achieve anonymity or intimacy"* (Steeves, 2014, p. 6).

Research shows that children react to the monitoring of their online behaviour in ambivalent ways. Canadian early adolescents (aged 11-12) appreciate parental control software because it alerted them of bad language and poor behaviour. Older adolescents were more ambivalent towards these tools because they it helped them to self-regulate screen time and online behaviour but were also experienced as annoying and unnecessary (Steeves, 2014). Moreover, children also respond actively to digital monitoring when they circumvent parental control software (e.g., via VPNs) (Livingstone & Blum-Ross, 2020; Steeves et al., 2020; Trinity McQueen, 2018). Strikingly, (early) adolescents who were not subjected to routine social media monitoring felt comfortable to discuss online incidents with their parents, which indicates a need to foster trust in parent-child relationships (Bennett et al., 2014).

Trust, communication, trust and media literacy

The moral assumptions underlying family surveillance revolve around trust. Trust in society, in the people around a child, in the parent, and in the child (Rooney, 2010). Trust enables children to handle the inevitable risks that life brings, and parental monitoring tools can be detrimental to this process. As Rooney, states *"without a surveillance gaze, children have the opportunity to be trusted, to learn how to trust others, and perhaps to show others they can live up to this trust. Once the surveillance is in place, this opportunity is greatly reduced"* (Rooney, 2010, p. 354). Particularly, extensive monitoring can be detrimental for trusting relationships between parents and children (Marx & Steeves, 2010; Stattin & Kerr, 2000). Trusting relationships are based on the assumption that children can be trusted to make the right decisions and that they might make a few mistakes in this process (Livingstone & Blum-Ross, 2020). Such relationships also require that children feel comfortable with sharing information with their parent. Adolescents are often the source of information about their whereabouts and activities (Crouter & Head, 2002; Kerr et al., 2010; Stattin & Kerr, 2000). This indicates that open communication can take away the need for intrusive monitoring practices. Open communication is also crucial for supporting the development of media literacy. Many parents aim to elicit safe (digital) behaviour by teaching children about (in)appropriate online activities and how to act when unsafe situations occur and engaging in discussions about these topics. In other words, they help children develop media literacy and advance their skills to *"access, analyse, evaluate and create messages across a variety of contexts"* (Livingstone, 2004, p. 3). In order to support this process, experts deem it important for parents to keep up with the technologies and to start early with educating children about online risks (Marsh et al., 2017). Children also learn about privacy practices from family members, friends, experts, their own experiences, and formal channels such as school (Subramaniam et al., 2019).

In the Netherlands, many schools have media literacy initiatives around cyberbullying, cybersecurity, and privacy. Yet, as indicated in interviews with Belgian adolescents (whose context is somewhat comparable to Dutch education), they deem some of their teachers unfit because they are not knowledgeable about media (De Leyn et al., 2021). Dutch parents of young children (4 -12 years old) indicate that they feel responsible for educating their children about media, but also believe that schools have an important role in increasing media literacy and resilience. Moreover, Dutch parents consider themselves media savvy yet state that they need practical advice for educating their children about media (Opree et al., 2021; YoungWorks, 2014). Advancing media literacy can help children to become resilient in digital environments and can take away the need for parental monitoring practices. In this study, I investigate how parents and children experience family surveillance. The results section provides insights into the role of trust and communication in their everyday practices.

Research method: Family interviews

Parental monitoring offers a lens through which family dynamics can be analysed and it enables an exploration of how monitoring process shape family life (Nelson & Garey, 2009). This chapter is based on interviews with 11 parents and 11 children and follows a constructivist grounded theory design (Charmaz, 2014; Corbin & Strauss, 1990). The methodological details are discussed in Chapter 2 and the respondent overview is included in Appendix 4 which also indicates the family set-up and if interviews were conducted one-on-one and or together. Appendix 8 presents the interview guides about which one additional consideration is noteworthy to mention: I emphasised at the start that the goal of the interview was not to judge parenting style or to evaluate it, but to discuss their everyday practices around technology use in the family. This way, I aimed to reduce the chance of parents giving socially desirable answers to display *good parenting* (Mazmanian & Lanette, 2017). While this aspect cannot be fully disregarded, most parents opened up about their parenting struggles around family surveillance; some were even corrected by their children who pointed out parenting inconsistencies.

Results: Everyday experiences of family surveillance

This section presents the four main themes that resulted from the constructivist grounded theory analysis (the selective codes). The full codebook is included in Appendix 15. The first two themes discuss how parents and children experience family surveillance (RQ1) in their everyday *media repertoires*, and by *ensuring openness and establishing rules*. Two contrasting ways in which parents engage in digital monitoring practices (RQ2) are described in two themes. Some parents engage in digital monitoring practices to *provide safety and guidance* whereas other parents refrain from digital monitoring in order to *encourage freedom and trust*. The practices discussed by respondents in the following sections are not merely representative of specific families but broadly indicate how experiences and practices of family surveillance occur across parental styles and families.

Setting the scene: Media repertoires of interconnected families

Experiences of family surveillance are embedded in everyday media use and communication. Therefore, I first provide an overview of daily media and communication practices of children and parents. When it comes to digital communication within families, all families in this research have an active WhatsApp group conversation wherein they share pictures, discuss practicalities, and update each other. Apart from that, media uses of children are different from those of their parents. The media repertoires of parents revolve around social interactions, practicalities, and entertainment. As Joel (48) describes: *"What do I use my smartphone for? For almost everything nowadays, I think. For to-do lists, for my work, for photos. To take pictures, to use WhatsApp, for social media. To Google, to listen to music".* Lucy emphasises the practical nature of her parents' messaging practices:

> *"If they receive a message about something, it's something they have to arrange at work or for sports or health or whatever. Just parenting stuff. And if someone texts me, it's more like oh, look at this seal I've seen laughing. That's not, it's not like oh, that's important, it's more about entertainment."* (Lucy, 15)

Furthermore, many parents actively try to keep up with the (social) media their children use. Some parents look up information about particular apps to inventory potential risks and others actively use social media. E.g., Nadia (42), a single mother of Ellie (12), explains: *"I just like to relate to her experiences. So, I also have a TikTok account and I uh, like to use Snapchat…I think it's very important to eh, go along".*

The media repertoires of early adolescents revolve around entertainment, multitasking, and many social interactions. The most often mentioned media practices were playing games, watching, and posting videos and interacting via Instagram or TikTok, messaging via Snapchat and WhatsApp, watching or creating live-streams on Twitch, and streaming content on YouTube, Netflix, and Spotify. Many children have multiple devices at their disposal and are used to engaging in more than one practice simultaneously. Jill (13) provides an example of multitasking: *"Sometimes I have a video call with my friend. Then we, eh, share our screens, for example when we are doing some online shopping".* Jill's practice also illustrates the social aspect of children's media repertoires. Most early adolescents indicated that digital social interactions gained importance during the Covid-19 lock-down situations when children could not, or less often, interact with their friends face-to-face.

Interestingly, early adolescents display a high awareness of digital media risks and provide many examples of resilient and careful behaviour.

For example, they develop strategies to screen unknown contacts and requests. If an unknown contact messages Scott (14) via WhatsApp: *"I first check who it is and if I know that person. And if I don't know him, I'd probably block him".* Similarly, when unfamiliar people start following Jasmin (12) on her public TikTok profile, she screens their accounts: *"And if I see that people are mean towards other people, or eh, people who say unkind things or do weird things, I think: 'What are you doing? Why are you following me?' And then I block them".* Moreover, early adolescents show awareness of the potential risks of sharing personal information or pictures via messaging apps and social media. Jill (13) often refrains from sending pictures via WhatsApp *"because they will stay in the chat for ever"* and Naomi (12) sometimes sends pictures but instructs her friends clearly: *"Then I just say: 'you can keep them, but you cannot share them'".*

Children's practices to protect their online privacy and safety showcase their ability to use, analyse, and evaluate digital media – their media literacy (Livingstone, 2004). Existing research describes how children develop media literacy on the basis of different sources (Marsh et al., 2017; Subramaniam et al., 2019). Early adolescents mentioned (the experiences of) friends, parents and other family members, school, media, and their own experiences as sources of information about safe online behaviour. Remarkably, echoing Subramaniam et al. (2019), parents not only educate children but this also happens the other way around. Abby (39) describes how her son (14) informs his sister and mother about media risks he learns about via social media and online videos: *"He watches, you have several of those short documentaries, especially on YouTube, where people, say, ethical hackers, show what the consequences are…So he's really like: 'Watch out, because yeah, you never know who's behind it.'"* Whereas school is often mentioned as a source of information, the quality and usefulness of this information is questioned by early adolescents, mirroring the findings of De Leyn et al. (2021). Scott (14) describes a social media lesson at school: "*It wasn't all that special. Just things you can think of yourself. That you shouldn't put your uh- nudes on your Insta or something".* Evidently, children develop media literacy based on multiple sources; schools form ambiguous, family members reciprocal, and social media paradoxical sources.

Ensuring openness and establishing rules

Whether they engage in digital parental monitoring or not, all parents shared similar values regarding family communication about digital practices. Family surveillance is enacted via conversations about media that allow parents to collect information about, and to control their children’s media use. More specifically, all parents and children mentioned that they regularly engage in open conversations about media use and risks, and that rules are established to ensure careful digital behaviour. The most often mentioned risk discussed in families is encountering strangers with bad intentions. Faith shares how she interprets her father’s cautions:

> Faith (11): “*If we click on a link, then our father becomes [angry], and gives a three-hour long sermon. And I’m not interested in that.*”
> Interviewer: *“And what is he preaching about?”*
> Faith: *“About dirty old men on the Internet. Or that they are going to hack you. And then they’re going to steal money from you, or something.”*

Other risks that were discussed in families concern cyberbullying, the digital collection of personal and behavioural data, social media’s focus on appearance, social media and game addictions, cybersecurity threats like phishing, inappropriate content, disinformation, sharing pictures. Families established rules informed by these risks. The most often mentioned rules concern social media use. Parents require children to set their TikTok and other social media accounts on private and prohibit them to post pictures or videos that are considered too sexy. Fiona (44) states: *“So you can’t, in the summer in your bikini, make videos and post them on TikTok. So, we don’t want that. We’re just very clear about that, you’re not going to give rise to people with wrong ideas”.* Moreover, open conversations about media use often revolve around content children encounter and what they post on social media. Some children that are active on social media show their posts to their parents. Jill (13) for example states that her parents do not have a TikTok account, “*but if I have a new TikTok, I often show it”.*

Many families discuss digital incidents, such as when children are approached by strangers, receive or see hateful messages on TikTok or Instagram, visit inappropriate websites, or receive inappropriate messages in group conversations on WhatsApp. The latter for instance happened to respondents Naomi (12) and Ellie (12) who encountered antisemitic and violent images in school-related WhatsApp group conversations. Another type of incident is when children forward pictures they receive from friends to others, this can lead to conflicts. Without getting into details, Greta (43) describes an incident that revolved around a friend's picture: *"Jack also had an experience of doing something he deeply regretted. And we solved that too, but he will never do that again".* Jack (13) responds: "*I found it very difficult to say it to you,"* to which Greta adds: *"But in the end he did. And then we solved it…Sometimes they have to learn the hard way, you know".* This example shows how Greta want to ensure that her children approach her when they have a problem or made a mistake.

The conversational practices discussed by the respondents indicate that in many families most knowledge of children's digital interactions and media use are based on self-disclosure of information. Family surveillance is visible in how parents aim to control and influence their children's media practices, risk awareness, and resilience by establishing rules and having open conversations about media use. The findings provide examples of how adolescents form an important source of information for family surveillance which supports research about parental monitoring (Crouter & Head, 2002; Kerr et al., 2010; Kurz, 2009; Stattin & Kerr, 2000). The following sections add to these studies by providing insights into two distinctly different approaches to digital parental monitoring that both go hand in hand with open conversations about media use and rules.

Parental monitoring practices: two sets of practices

The analysis resulted in two contrasting clusters of codes that provide an answer to the second research question. Parents engage in digital monitoring practices in different ways. First, in some families parental monitoring practices are motivated by the goal of safeguarding and providing guidance. In contrast, other families do not engage in monitoring practices but prioritise their children's freedom and trust.

Providing safety and guidance

Some families actively monitor their children's whereabouts, interactions, and activities. The most often mentioned monitoring technologies are location tracking apps or services, student tracking systems (provided by schools to track progress and attendance), and tools to monitor (and restrict) Wi-Fi use. Some parents engage in more elementary monitoring practices such as accessing their child's smartphone to check their messaging apps and social media or restricting screen time by taking their smartphone away.

In this section, I discuss the forms of parental surveillance that were most common among the respondents and concerned locations, screen time, digital behaviour, and educational progress. These strategies are embedded in everyday family life and, adding to research that indicates how parental monitoring practices can cause tensions (Nelson & Garey, 2009), this section shows that children not only resist monitoring by expressing their discomfort, but that they also develop strategies to circumvent monitoring. First, four families make use of location tracking apps, some do this on a daily basis while others only use them occasionally. Nadia (42) started using Live360 when Ellie (12) started high school:

> *"I installed that when she went to high school so I could watch her ride her bike. Because it shows how many kilometres per hour she bikes, and where. With the initial intention of gosh, if she can't find her way, I can watch her and help her navigate. Um, and that I know, okay, she's going home now, because then I get a notification like 'she's leaving school now'...But that's also the, well, what I just told you, the only thing we use it for. Actually, a bit for emergencies."* (Nadia, 42)

Paul (42) also regularly checks where Parker (13) is: *"But it's not a controlling function, erm, it's more of a handy feature, a reassuring feature".* Nadia's and Paul's quotes indicate that reassurance and safety are the main motivation for using location tracking apps, echoing Ervasti et al. (2016). Ellie (12) does not mind her mother's monitoring practices:

"I'm not going to secret spy meetings or anything. But, eh, I don't mind it... My friend said: 'well, I would not want my mother to always see where I am'. But eh, I don't really have a problem with that" (Ellie, 12)

Interestingly, in some families, family surveillance has a reciprocal character. Jasmin (13) shares; *"sometimes I want to know, for instance, oh, at what time will we have dinner? How far is mom away from her work?"* Jasmin not only checks the location of her mother, but her parents can also check each other's location and use this around dinner time: "*When I crossed the [name of bridge], then they know I'll be home in fifteen minutes and then they can bring potatoes to boil, so to speak".* (Camila, 45) The reciprocal nature of location tracking (as discussed by two families) further underscores how location tracking can be embedded in everyday family life.

Second, as indicated in existing research, managing screen time is a universal challenge for parents (Marsh et al., 2017; Mazmanian & Lanette, 2017; Nikken, 2021). Some of the respondents share that they chose to let go of restrictions when their children became early adolescents, or at least to be more flexible. Other respondents disclose that the lock-downs caused by Covid-19 made it even harder to manage screen time because children had fewer other activities. However, multiple families in this research maintain strict rules and restrictions. Grace and Oscar use screen time restriction as punishment: *"Taking your phone away is more because you're not listening, you're using it for too long and you're not doing the things that we asked you, so it's a measure"* (Grace, 43). For Lucy, this is a severe measure:

> *"For some things I need my phone or my laptop, for example for school, now also for work. Then it's kind of, if you take my phone away, you're really just taking something away that, I think, that, that's the only thing, uh, that makes this day and age bearable. And especially during Covid [restrictions], if, or during the holidays, when all my friends are gone, then what should I do? Going outside in the cold to play a game? Should I play checkers on my own?"* (Lucy, 15)

Lucy's response indicates that she feels her parents underestimate the importance of her phone. In addition to early adolescents voicing complaints about screen time restrictions, other respondents describe how children circumvent restrictions. Jasmin (13) resists the rule that she is not allowed to keep her smartphone in her bedroom during the night. Her mother Camila (45) states: *"If Jasmin gets the chance, and I forget to ask her [to leave her phone with her parents], she will hide it in her room".* In addition, Jack (13) describes how his friend avoids his own parents' screen time restrictions by visiting Jack in order to play games.

Third, parents can keep an eye on the media content, contacts and conduct of their children (Brisson-Boivin, 2018). Remarkably, this only happens occasionally in a few families and takes an elementary form (Marsh et al., 2017). Instead of using digital tools to monitor media use, parents access their child's phone to ensure they are not engaged in any inappropriate activities or interactions. Paul explains how he monitors the phone of his sons Tim (11) and Parker (13):

> *"I also have the access codes. Sometimes they change it, but then I just ask for the access code and they give it to me. Eh, because there are no secrets for me in that regard. At least, uh, I hope not. And so, I can see what sites they've visited, unless they've cleared it, then of course I don't know. Um, I know roughly what games they play, I know it's pretty harmless."* (Paul, 42)

This quote shows that Paul's monitoring practices mainly concern the content – what his children consume online (Brisson-Boivin, 2018). In a separate interview with both of Paul's sons, Tim (11) responds to this monitoring practice: *"It is safe, yeah, I think it is. When I do something, he can just open it and see it in my history".* While Tim does not mind his father's parental monitoring practices, some children react differently to the monitoring of their smartphones. Lydia (45) regularly accesses the smartphones of her children to check their messaging and social media conversations. The interview with Lydia and her foster children shows that this can cause tension:

> Lydia (45): *"And sometimes you just don't feel like it. Then you will not give your access code to me, right?*
> Eli (12) and Faith (11) simultaneously: *"Yeah"*

> Lydia: *"And that's especially if you're a little annoyed with me, isn't it?"*
> Eli: *"Yes, or if I forget. Because I still forgot to tell you the code."*
> Faith: *"Or [annoyed] with dad, he once wanted Eli's phone to watch something and then he deleted all the messages."*
> Eli: *"That's why he doesn't know my code anymore."*
> Lydia: *"No, but we agreed, you can have a phone but we can look into your phone at any time."*

The ambivalence in how early adolescents respond to the monitoring of their online behaviour was also visible in earlier research (Steeves, 2014). Eli's example of refusing to provide his access code is one of the ways our respondents avoided parental monitoring. Ellie (12) provides an additional example, she does not mind that her mother Nadia can see her posts and interactions on TikTok and Instagram, yet she sometimes avoids her mother's gaze: *"For instance, when my friends are acting crazy again, then there is Snapchat, and then I'll tell the girls: 'post it on Snapchat'. Um, because there, that's the only platform my mom can't see".*

Finally, our respondents describe practices around the monitoring of school progress. Student tracking systems (STSs) are used by almost all high schools in the Netherlands. Such systems have separate student and parent interfaces (web-based and mobile applications) where they can check schedules, homework, attendance, grades, and school messages ('Leerling & Ouder: Magister Web En Magister App', n.d.). Whereas almost all parents use STSs for messages or to occasionally check grades or attendances, some parents engage in more intensive monitoring practices. Jasmin's (13) mother Camila describes:

> *"I actually try to do it every day eh, especially because I also know that Jasmin finds it difficult to keep up…Maybe other kids get very good marks. Look, if Jasmin always comes home with eights and nines and sevens and so on, I'm really not going to check Magister [STS] all the time, because then I know you've got it under control."* (Camila, 45)

Camila uses the student tracking system to provide guidance in Jasmin's school work. She states that she wants to prevent that Jasmin's difficulty to keep up with schoolwork harms her education. Her quote also indicates that she plans to give Jasmin more freedom as soon as her grades improve. Jasmin (13) is ambivalent about the homework monitoring: "*Sometimes I find it a bit annoying. Um, but sometimes I do think, she does it to help me even though I don't want to realise it, but I do know that. I personally think that my friends' parents are probably a lot less strict".* Camila's monitoring practices lead to tensions and affect Jasmin's behaviour around homework. Similarly, for Lucy (15), her parents monitoring her STS enforces good behaviour because she refrains from skipping class: *"I know that if I were to skip school, that would make my parents angry. So, I'll go to class anyway, to do nothing there and just sit for an hour".*

Concluding, the discussions of monitoring practices illustrate that these are motivated by the urge to protect children and to safeguard and guide them. Digital monitoring practices occur in half of the families in this research and range from being fully embedded in everyday family life (such as in the families of Nadia, Paul, and Camila) to limited surveillance and restrictions (like Lydia and Grace and Oscar). It is noteworthy that some parents aim to find a balance between monitoring and providing freedom. Abby provides a clear example of how she engages in monitoring practices via student tracking systems but simultaneously wants to give her children the chance to make mistakes:

> *"Such a system is very nice, but you can follow everything. The moment a child is late or messes up in class or whatever, you see it. And actually, as a parent you shouldn't see that because of the system. You should hear that [from your child], because you have to build a relationship of trust…But once in a while it's okay to check the system, because then you at least know the situation."* (Abby, 39)

Encouraging freedom and trust

Abby found a balance between checking in on her children's school progress occasionally but providing them also the opportunity to approach her about an incident or grade. Instead, Fiona and George, Greta and

Jack, and Joel decided not to engage in digital monitoring practices. They often explain this decision by referring to their own childhood, Fiona (44) shares: *"My parents didn't know what I was up to either. Yeah, it's nice that you can have social control, but you don't necessarily have to take it. It's also about trust in your kids that you shouldn't lose, you know".* This quote highlights the importance of trust, a word that many parents mentioned as contrasting monitoring and controlling.

For Fiona and George, trust, freedom, and communication form the basis of their parenting style. This is also visible in how they trust their children to check in with them. George (42) explains: *"Usually they will let us know when they go somewhere, yesterday for instance, when they went outside…And as a child, I really liked to have such freedom. And I think it is important that you sometimes come home late".* Fiona adds: *"That's part of being a child, go on your own discovery and adventures. And not eh, that your mother or your father is constantly breathing down your neck. I don't think that's healthy either".*

When it comes to monitoring screen time, some parents are stricter than others. Greta (43) indicates that she let go of restricting how long Jack (13) played games on his smartphone. That that turned out well: *"We found a good balance. Look, if it, it the weather is horrible like yesterday, and it rains all the time, then, well, then I don't mind that he, for example, spends a lot of time with his phone. And uh, the next moment he goes outside again".* Similarly, some parents also trust their children to be careful and make the right decisions when it comes to online behaviour and content. Joel (48) refrains from monitoring what his adolescent sons watch online, which games they play, and how they interact online: *"At a certain point I knew well, Scott [14] and [eldest son of 16], they just handle it wisely. Or they will skip something when they think oh, you know, that's nasty".* These parents show that they prefer establishing trust to digital monitoring. These findings reflect Livingstone and Blum-Ross's (2020) description of trusting relationships wherein children can make mistakes. Joel also mentions this when he explains that he never checks his sons student tracking systems:

> *“I think that’s such a horrible thing. Then I think, I used to get really low grades at school, you know. Well, I couldn’t imagine my parents being able to see that. And then I think, in the end everything turned out all right…and I’d much rather they just tell themselves that they [received a low grade]- because you know, when something like that happens, they hate it themselves, you know. And even if I don’t hear about it and they err, eh, they’ll fix it.”* (Joel, 48)

Abby (39) emphasises the importance of giving children the freedom to develop themselves: *“It is especially important in puberty to find your own path, and your own shoes, and take your steps”.* In families where the parents that decided not to engage in digital monitoring practices, trust and freedom prevail against monitoring. Their practices show positive expressions of confidence in children (Rooney, 2010).

Conclusion: Situated family surveillance practices

By interviewing both children and their parents, I provide a complete account of everyday experiences of family surveillance. This chapter contributes to existing research about parental monitoring and family surveillance in four ways.

First, the actual practices of parents and children indicate that family surveillance can only be understood in a context of nuanced everyday technology use. The practices of parents who focus on safeguarding and guiding their children can be seen as fitting a state of hypervigilance characterised by little regard of children’s privacy, self-determination, and no presumption of innocence (Katz, 2001), a lack of trust and no room for negotiations (Rooney, 2010), and by the assumption that children are incompetent (Simpson, 2014). However, it became clear that the use of digital monitoring tools goes together with open discussions about online risks, practices, and incidents. This shows that even when parents monitor their children, there is still room for children to develop agency and to earn their parents’ trust. Moreover, the responses of children to their parents’ monitoring practices as well as their resilient digital practices show that early adolescents also play a role in resisting this alleged state of hypervigilance and that they demand and create freedom to protect their privacy and determine their own path. Their strategies to challenge and circumvent parental monitoring provide a clear example of how they are actively becoming more autonomous from parents or guardians. This does not mean that parental monitoring technologies should not be critically assessed, but rather that they **should be studied in the context of broader constellations of media and communication practices within families.**

Second, when it comes to digital resilience, (early) adolescents showed an awareness of digital risks that is fully integrated in their daily practices. Awareness and resilience were informed by personal experiences and discussions with peers and family members (which entailed two-way flows of information). Whereas the interviews showed that most parents find open conversations about technology and digital incidents important, these findings further emphasise the need for open conversations about technology. Children's accounts of where and how they develop resilience highlight the need to not only discuss incidents, risks, and rules but to **include digital media use in casual conversations.**

Third, family surveillance practices entail lateral surveillance, i.e. interpersonal monitoring (Andrejevic, 2002; Trottier, 2012), and in some cases this is a reciprocal process. In multiple families where monitoring was embedded in everyday practices, the respondents indicated that children also check the location of their parents (and the parents of one another). These findings indicate that my earlier conceptualisation of family surveillance needs to be broadened. From limited to a focus on children, the interviews inform a conceptualization, the interviews inform a conceptualisation of **family surveillance as a lateral process of keeping track of the digital and non-digital activities and associations of family members.** This reciprocal nature of family surveillance deserves more attention in future research.

Finally, a more indirect conclusion can be drawn from the way personal histories of parents form an important context for parental monitoring practices. **Family surveillance practices are situated not only in current family settings but also within individual and collective family histories.** Almost all parents compare the life of their child to their own upbringing when they reflect on the freedom they enjoyed themselves and on how their children have more media and devices at their disposal. For some parents, these reflections substantiated their motivation of not using digital monitoring tools, whereas other parents felt that digital monitoring practices fit within the current age and time. Two parents explicitly expressed that they found it enlightening to discuss their own youth, and said it helped them reflect on how they bring up their children. A lesson that can be drawn here is that in order to elicit productive conversations about family surveillance and to establish mutual understanding between parents and children, it is helpful for parents to reflect on their own childhood.

Limitations and suggestions for future research

This chapter provides an in-depth and nuanced account of parental monitoring in Dutch families but is also limited in several ways. The small sample size is not representative for a larger Dutch or international population. However, the diversity of findings within these nine families reveals a range of challenges, practices and considerations around parental monitoring that are expected to be visible in other populations as well. Future research could address family surveillance practices in other countries, and as most research focuses on the UK and North America, it would be good to expand the scope to other parts of the world. Moreover, this research took place in May and June of 2021, when a second lock-down because of the Covid-19 pandemic was on its return in the Netherlands (the restrictions were lessened from a full lock-down to general social distancing rules). Whereas this unique context provided additional insights into how parents manage screen time and into the role smartphones play in the social lives of (early) adolescents, some of the findings might have been different in a time without Covid-19 restrictions. Therefore, follow-up research could also focus on the longitudinal and contextual dimensions of family surveillance practices.

Chapter 9

Conclusion
Sociomaterial privacy and surveillance negotiations

Everyday experiences of privacy and surveillance are inherently contradictory and fickle. The introductory chapter describes how my own experiences of privacy and surveillance entail considerations of protecting my personal time, space, and information when I make use of various platform-based technologies and services. Similarly, the cross-contextual privacy and surveillance practices of this dissertation's respondents are far from consistent or homogeneous. Yet, in answer to the overarching research question: *How do people experience privacy and surveillance in their everyday practices?*, respondents have one thing in common. That is, people **experience privacy and surveillance through sociomaterial negotiations of appropriate forms of monitoring.** This answer includes three aspects that need to be clarified. First, individuals negotiate what **they deem appropriate** forms of monitoring. To illustrate, chapter 8 shows how (early) adolescents experience family surveillance. Once they become aware of parental monitoring, adolescents decide whether they find this appropriate (such negotiations can happen consciously as well as unconsciously). Adolescents can respond to family surveillance by accepting it because they find it appropriate or, when monitoring practices are considered inappropriate, they can try to protect their privacy by circumventing monitored (digital) spaces or confronting their parents.

The second aspect that needs clarification relates to the fact that there are many forms of monitoring – including commercial, family, governmental, and lateral (peer-to-peer) surveillance. Because of the multidimensional nature of surveillance, monitoring can best be understood as **contextualised surveillance practices.** Resembling privacy as contextual integrity (Nissenbaum, 2004, 2010, 2019), surveillance negotiations are context-dependent and based on norms of appropriateness.

The empirical research in this dissertation shows that people negotiate what they deem appropriate and inappropriate surveillance practices. Norms around appropriateness are context dependent. For example, respondents perceive parental monitoring in a different manner than commercial surveillance by household IPA platforms. It is important to note though, that the contexts wherein people experience surveillance practices are not fixed. Instead, privacy and surveillance negotiations most often take place against a backdrop of digital/physical context collapse (Pagh, 2020). All the practices that respondents discuss have online and offline counterparts, and their everyday practices entail boundaries between digital and physical contexts that often and easily collapse. Family surveillance practices can for instance take place in a living room (physical context) when parents ask their child what type of content they are streaming on their smartphone (digital context).

Third, **the sociomaterial nature of negotiations** needs to be explained. Returning to the example of family surveillance, adolescents' socially oriented negotiations are enacted through material elements like smartphones, social media interactions, and digital or physical conversations with parents. The sociomaterial nature of privacy and surveillance negotiations is clarified in more detail in the next section of this conclusion. Subsequently, inequality and a lack of transparency are presented as two key concerns that complicate everyday negotiations of privacy and surveillance. Afterwards, I present an overview of how these findings contribute to existing literature, their practical implications and take-aways, and the empirical lessons they provide. Finally, I reflect on the limitations of my study and provide suggestions for future research.

Sociomaterial negotiations of contextualised monitoring

Negotiations of privacy and surveillance are sociomaterial in nature, which becomes clear in how people experience as well as in how they respond to them. This research shows that when privacy risks, boundaries, and infringements become explicit, people negotiate the (in) appropriateness of contextualised surveillance practices. For example, when people warn their neighbours about incidents like house break-ins or suspicious activity, they make these risks tangible in the form of WhatsApp messages. Materialised risks in a digital WhatsApp context prompt social negotiations in the physical contexts of participants' homes and the neighbourhood. These risks often activate other neighbours into participating in (vigilant) surveillance practices to safeguard, monitor, and protect their house and their neighbourhood. Besides, materialised risks also influence citizen's negotiations in contrasting manners; some respondents feel safer when they know that the materialised risks lead to better protection of the neighbourhood while others experience anxiety when they become aware of the risks that can threaten their safety. The WNCP practices discussed in Chapters 3 and 4 indicate how materialised risks lead to tangible negotiations which instigate surveillance practices and influence the well-being of people.

In the family contexts presented in chapter 8, surveillance is negotiated through sociomaterial practices of parents and children. Parents can take their children's smartphone and unlock them to check their smartphone use, or they can use digital applications to track their children's location or online behaviour. Digital interfaces form material artifacts of family surveillance. In negotiations of the appropriateness of such surveillance practices, early adolescents respond to physical and digital surveillance in different ways. One girl, for example, hides her actual phone to not have to hand it to her mother, whereas another girl avoids digital monitoring and uses Snapchat as an unsupervised communication channel. By discussing family surveillance negotiations within families, the respondents provide insights into how devices as well as digital interfaces make up the material dimensions of surveillance practices and privacy-preserving activities.

When it comes to privacy, the sociomateriality of risks influences how concerned people are about household IPAs. Surveillance with physical privacy risks is considered less appropriate than commercial surveillance. To illustrate, in Chapter 7 respondents describe insufficient or failing device security as a risk of hackers using their device to plan house break-ins (a material and tangible threat) far more often than risks of identity theft (a less tangible threat). Most respondents bring up immediate and material risks as reasons for not using household IPAs or restricting their use (by muting or unplugging the device). In contrast, they share more pragmatic attitudes towards hypothetical and intangible risks around data collection. This indicates that people feel a stronger motivation to protect their privacy when they experience tangible threats.

The tangibility of privacy and surveillance negotiations is also clearly visible in boundary management of presence, contexts, and personal information. Boundaries around personal information are largely unnoticeable but become tangible when incidents occur or when people directly experience the negative consequences of personal information disclosures. Such incidents reveal inappropriate consequences and form reasons to install stronger boundaries and to change behaviour (in light of communication privacy management, incidents form catalyst privacy criteria, Petronio, 2012). The same can be said for negotiations of boundaries between absence and presence and between different contexts. People will become aware of their boundaries when these are compromised, e.g., when they begin to experience online communication as an intrusion to their offline context and start negotiating absence and presence more consciously.

Furthermore, privacy negotiations via boundary work also become tangible via material objects. Boundaries become most prevalent when people leave their laptops in their office at the end of a workday, or if they put their smartphones away when they spend time with friends or family. Digital objects such as the interfaces of messaging apps, smartphone *do not disturb* and *silent* modes, particular sound settings, and WhatsApp's *blue checks* and *last seen* can also form tangible indications of boundary work practices. By revealing the material elements of boundary management, the focus can shift from the consequences of privacy breaches (in the form of inappropriate tensions and boundary turbulence) to conscious means of sculpting and protecting personal boundaries.

Altogether, these findings illustrate how tangible risks, devices, applications, objects, settings, and interfaces form crucial components in negotiations of appropriate surveillance practices. Because privacy and surveillance become pressing when they are seen as tangible acts of negotiation, the sociomaterial nature of such negotiations needs to be addressed. The experiences of the respondents make clear that there are two concerns that complicate negotiations of appropriate monitoring practices: inequality in digital skills and decision-making, and a lack of awareness. The next two sections explain how these concerns constrain people in their everyday negotiations of privacy and surveillance.

Inequality in sociomaterial privacy and surveillance negotiations

Respondents' experiences of privacy and surveillance indicate that **inequality in digital skills and decision-making leads to power imbalances in surveillance and privacy negotiations**. For example, when parents monitor children, they hold power over them, power that they exercise via family surveillance tools. Whereas children can negotiate parental monitoring, power inequalities between them and their parents might hinder them in carrying out decisions that stop the monitoring practices. Before I present other examples of inequalities in privacy and surveillance negotiations, the role of power in practices needs to be reviewed. Watson (2016) states that human relations are essentially power relations in networks of practices. Power can be an effect of practices when the social location of an actor in relational networks of practices offers the means to shape the actions of others. To put it differently, power is embedded in practices in the relations between meaning, competence, and material dimensions (as discussed in Chapter 2 based on Shove et al., 2012).

This can also be illustrated with the example of family surveillance. Family surveillance practices entail material dimensions: parents, children, and monitoring tools like location tracking apps, meaning in the purpose of safeguarding children, and competence in knowledge of how to use monitoring tools. When these elements interact and surveillance practices take place, power flows in the relations between parents and children. In this process, inequalities become visible. When parents decide to engage in family surveillance practices and children have no say in the matter, power flows from parents to children. (In)equalities in surveillance and privacy negotiations are intrinsically related to power whereby digital skills and decision-making form the two main concerns.

First, the varying levels of digital skills among technology users in this research cause inequality in surveillance and privacy practices. This is the case for participants in WhatsApp group conversations in work, family, WNCP, and many other relational contexts. Limited knowledge about WhatsApp settings can create inequalities in opportunities to monitor others, whereas it can also lead to a lack of awareness of lateral surveillance by others. It takes some advanced knowledge to check if and when others have read a message (users need to open *message* *information* by swiping or by selecting a message). A power imbalance occurs when less digitally literate participants of group conversations are not aware of these options while others actively use them – they are less capable of actively engaging in (preventing) surveillance practices. Such inequalities can lead to tensions between participants (for instance when they are reprimanded for not responding to a message that they have read).

Similarly, digital literacy also plays a role in smart speaker users' ability to negotiate appropriate forms of surveillance practices because it influences how they can protect their privacy and avoid or circumvent commercial surveillance. Most household IPAs have a *mute* function to temporarily put the device in a non-listening mode. However, not all users are aware of this option to disable auditory surveillance (naturally, fully unplugging the device would block any form of auditory surveillance, but restarting the devices requires more time and effort than pressing a single button). In addition, unequal access to information and knowledge is at stake when one person in a household (in families most often a parent) has access to and control over smart device settings, connections, and insights into the commands and uses of all household members. More advanced knowledge is required to connect multiple accounts and to enable the voice recognition of different family members. Yet, a lack of customisation can lead to a power imbalance in intimate contexts. Household members are constrained in their ability to negotiate surveillance practices when they are not able to access device information. Interestingly, children sometimes prove to be more knowledgeable about device settings than their parents, which reverses power imbalance issues around digital literacy and technology use.

Second, **inequalities exist around decision-making** and curb people in their autonomy to adequately negotiate appropriate forms of surveillance and sculpt privacy protection. In work contexts, inequality can determine to what extent employees can freely engage in boundary work practices to manage their privacy (Nippert-Eng, 1996a) and personal information (Petronio, 2012). Employees do not have full autonomy to make decisions about when and how workplace communication takes place. Managers and companies can expect communication that is not always voluntary or accompanied by implicit expectations, for example, when employees are included in group conversations without their consent or are expected to answer email during their weekends.

Whereas work hierarchies and work situations often have power inequalities as a formal basis (naturally, a managerial function gives more power to make decisions than a junior position), such power dynamics transcend into more personal contexts when it comes to communicative practices. When workplace communication takes place on platforms or devices with a not solely work-related purpose, employees lack the power to negotiate boundaries themselves. In other words, employees can be limited in their autonomy to sculpt boundaries between relational contexts when workplace communication takes place on personal devices or via platforms where they also have private interactions. Moreover, employees can feel forced to connect to managers or colleagues via their personal social media. This consequently also limits their decision-making abilities in self-disclosure practices and forces them to be subjected to social media surveillance. Again, they cannot properly negotiate what forms of (lateral) surveillance they deem appropriate, and what forms of surveillance they want to shield themselves from.

A similar dynamic can be seen in families, where natural power divisions between parents and children can constrain the autonomy of children in negotiating boundaries around their personal information, conversations, and relational contexts. Overall, it becomes increasingly clear that inequalities in decision-making and digital literacy amplify or create power imbalances across contexts. These limit the negotiating potentials of people to establish and act according to what they deem appropriate forms of privacy and surveillance.

A lack of transparency around surveillance practices

Sociomaterial negotiations of privacy and surveillance are also constrained when people do not have the information needed to exercise control over monitoring practices. More precisely, **a lack of transparency leads to a lack of control over three forms of surveillance: lateral, family, and commercial monitoring.** Transparency is often seen as necessary for limiting surveillance, and this research shows what is at stake when people are not able to adequately negotiate the appropriateness of surveillance around these three forms of surveillance. First, a lack of transparency about lateral surveillance leads to problematic disparities between people. For instance, in the context of monitoring practices in neighbourhoods, many WNCP groups are not transparent about who participates and how to participate appropriately in lateral surveillance and policing practices. Not only does this mean that uninformed citizens can be subjected to lateral surveillance practices without their consent, it also leads to opaque communication networks wherein participants might not be aware that police or municipal actors have access to their WNCP information. Moreover, appropriate forms of surveillance activities by neighbours are actively negotiated, and participants often reprimand others face-to-face or in the WhatsApp group conversations. These examples show that a lack of transparency around the existence and conduct of WNCP practices can lead to interpersonal tensions and toxic neighbourhood dynamics.

Further, in workplace contexts, employees are not always aware when they are subjected to workplace surveillance or lateral surveillance. When colleagues, business relations, or managers look up an employee on social media or check if they have read their message on WhatsApp, employees are subject of surveillance practices unknown to them. This takes away their autonomy to actively negotiate the appropriateness of lateral surveillance practices in the workplace until such surveillance becomes visible. Surveillance can become visible when the surveilling agents respond to what they have monitored by making a social media comment or by calling out a person on something they shared online. Such practices breach the privacy of employees which can affect their wellbeing, create tensions in the workplace, and harm interpersonal relations.

Second, this research also emphasises the consequences of unclear communication about family surveillance. Whereas in some families, children are informed about the monitoring practices of their parents (and sometimes even also monitor the locations of their parents in a reciprocal manner), this is not the case in all families. It is problematic that some children are not aware of family surveillance because this takes away their chance to negotiate monitoring practices. When parents are not open about monitoring practices, this can decrease their children's trust, while trust is crucial for open parent-child communication (Crouter & Head, 2002). In community, workplace, and family contexts, a lack of transparency around monitoring goes hand in hand with a problematic lack of consent of the subjects to these surveillance practices. When people do not have the chance to negotiate the appropriateness of such practices, this can be detrimental to interpersonal dynamics and relations.

Third, users of digital technologies have to deal with a lack of transparency around institutional and commercial surveillance concerning data collection, processing, and sharing. The use of interconnected (smart) technologies, social media, and messaging apps is only possible when users provide data and, in most cases, they have only limited opportunities to control their own data. It is unclear how platform companies use personal (meta)data and with which third parties data are shared for what purposes. Household IPA users automatically opt-in to commercial surveillance practices. Their concerns about platform data collection are intrinsically connected to unequal access to personal and behavioural information. Users can access a history of the commands and services they used but lack insight into which meta data are collected, processed, and shared by household IPA platforms. Furthermore, they can only use smart devices if they provide at least some basic personal information. Respondents in this research feel uncomfortable with platform data collection and fail to see ways of using such technologies without being subjected to platform-based commercial surveillance. Such feelings reiterate concerns around the power and commercial interests of platforms (Pridmore et al., 2019; Van Dijck et al., 2018; Zuboff, 2019). It is important to note that digital communication practices are tied to the same premises and that users face a similar lack of transparency around which (meta)data are collected and processed. WhatsApp is owned by Facebook and the terms of service are revised often. Throughout this dissertation research it became clear that a lack of transparency around lateral, family, and commercial surveillance leads to tensions and concerns. What is more, when people are not aware of surveillance, this limits them in negotiating their informational, spatial, communicational, proprietary, associational, and behavioural privacy (Koops et al., 2016).

Practical implications and suggestions

There are different ways to transform these concerns into practical suggestions for personal, social, and regulatory efforts to increase control over and awareness of privacy and surveillance. A radical response to issues around equality and transparency would require changing the underlying (power) structures; by redesigning WNCP structures in an open and fully transparent process or discarding the platformised basis of all technology-based practices by using alternative technologies (such as using Signal or Telegram instead of WhatsApp). However, these propositions are less feasible, given the actual everyday practices the respondents describe. A regulatory approach would focus on how governments can mandate better privacy protection and reduce surveillance. Yet, while regulation is important and should always be part of solving issues around privacy and surveillance, regulatory solutions often overlook the positive experiences of everyday technology practices. In order to maintain a nuanced approach to sociomaterial negotiations of privacy and surveillance practices in everyday life, I will provide a set of pragmatic suggestions. These suggestions build on communication and tangibility in order to increase equality and transparency around, awareness of, and resilience in privacy and surveillance practices.

First, **open communication is crucial in increasing equality and transparency around interpersonal, family, and commercial surveillance**. To increase equality in WNCP practices, moderators should put more effort into communicating who participates in the WNCP groups (neighbourhood, police, and municipality actors) towards members. Also, moderators need to not only provide ample opportunities for (new) neighbours to get involved but they should also keep neighbours who chose not to join the WhatsApp conversation informed about the WNCP practices within their community. This way, disparities between surveilling neighbours and neighbours that are subjected to surveillance can be partially leveled by WNCP moderator-initiated communication. In workplaces, inequalities in decision-making about boundary management can also be decreased via communication; open conversations between managers and employees can explore the needs and wants of different actors around digital workplace communication. Employees should have a say in how they want to negotiate privacy and surveillance around their availability and (informational) boundaries. Particularly, the global Covid-19 pandemic made working from home more common (if not the norm) for many knowledge workers. This makes the need for open communication around digital workplace communication, privacy boundaries, and surveillance practices even more pressing.

Similarly, the open discussions about media use that take place in many families can form a good basis for discussions about family surveillance and privacy negotiations. If children have full knowledge about when their parents monitor them, they can openly reflect on their personal experiences of monitoring, and clear agreements can potentially replace certain forms of parental monitoring. Besides, the reciprocal nature of location tracking in some families might even form an example of how to approach parental monitoring in a more equal manner. And in the contexts of household IPAs, all household members should be involved in open communication about who interacts (people as well as technologies) for what purpose, how, when, and in which interconnected contexts. More specifically, it might be helpful for household members to discuss which appliances, accounts, and services are connected to smart devices and how this enables commercial surveillance. This way, users can share knowledge about muting devices, privacy settings, and insights into everyday uses.

Second, I suggest that **tangibility is key to increasing awareness of and resilience in privacy and surveillance practices**. As indicated in Chapter 8, it is recommended for parents to not only discuss privacy and surveillance in isolated conversations aimed at improving awareness, but also to discuss privacy and surveillance negotiations more often in casual family conversations. This way, children get accustomed to talking about these topics and might become more aware of the consequences of their everyday technology use and appropriate forms of contextualised privacy and surveillance practices. Such open conversations can be informed by the aforementioned finding that the more tangible privacy and surveillance are perceived, the more they seem to motivate people to adopt privacy protection measures. Therefore, I advise parents and educators to use metaphors when they discuss privacy and surveillance. To illustrate, digital communication via messaging apps can be compared with writing letters, and the question can be posed how a child would react if someone opens their letter and shares the content with others; or closing bedroom curtains at night during a sleepover with friends can be a metaphor for being visible on social media where private accounts form curtains that only reveal information to a select group of contacts. Such metaphors almost always fall short of grasping the full complexity of privacy or surveillance, but they are useful in acknowledging the urgency of privacy and surveillance in everyday contexts.

Similarly, in the context of boundary work, it is useful for parents, educators, and managers to make boundary sculpting options tangible. Boundary sculpting practices entail most often unconscious processes, and people only become aware of these practices when friction occurs or boundaries are breached. Boundary work is highly important for experiences of privacy and for helping people feel free to be themselves without any distractions, influences, or pressure. Therefore, to increase boundary sculpting skills and awareness in family, school, and workplace contexts, it might be helpful to discuss the options people have to negotiate transparency. It is important that people go beyond the default visibility that most social media and communication platforms offer. More precisely, it can be useful to discuss the consequences and options around *blue checks* and the *last seen* setting on WhatsApp, to map expectations and options for availability in workplace communication channels (such as Microsoft Teams, Slack, and email), and to teach children about the *do not disturb* mode to enable them to create moments without pressure from notifications and distractions from endless group chat conversations.

Also, the use of tangibility as a tool to increase awareness about privacy and surveillance can also help to increase resilience in everyday uses of (communication) technologies. Solutions based on the tangibility of information flows and functionalities can be of assistance here, such as tools that highlight personal information in order to make users aware of risky digital disclosures (e.g., the PII filter browser add-on alerts users when they type in sensitive information like email addresses or phone numbers, see SIDN fonds, n.d.). Furthermore, similar to many laptops, some smartphone cameras are equipped with a notification light to let the user know when they are activated and when the user is being watched. These tools can form an example for technology producers and platform companies which can put efforts into making risky behaviour tangible and visualising data collection. They can, for example, use symbols instead of long winding user agreements (on some smartphones and apps this is already done to some extent), add colour indications for different risks, or probe users with clear cut, short, and visual opt-in and opt-out interfaces at the start and during the use of apps. In sum, making things tangible is key to successful efforts to improve privacy and surveillance awareness and resilience and to further adequate and well-informed privacy and surveillance negotiations.

Theoretical lessons and contributions

In the empirical Chapters 3-8, I present the contributions of this research to particular bodies of existing research, such as boundary theory (Nippert-Eng, 1996a), participatory policing (Larsson, 2017), parental monitoring (Kerr et al., 2010; Marx & Steeves, 2010), communication privacy management theory (Petronio, 2012), and research about privacy and household IPAs (Lau et al., 2018; Liao et al., 2019; Lutz & Newlands, 2021). On top of that, the findings of this dissertation also provide overarching contributions to privacy and surveillance research.

First, this dissertation presents many cases of lateral surveillance in, amongst others, neighbourhood watchfulness practices, workplace settings, and family contexts. As discussed in the introduction, lateral surveillance (also described as peer-to-peer, interpersonal, and social surveillance or co-veillance) relates to horizontal surveillance practices between individuals (Andrejevic, 2002; Lee et al., 2017; Mann, 2016; Manokha, 2018; Marwick, 2012; Trottier, 2012). Although the circumstances and consequences of lateral surveillance practices in this dissertation differ per situation, all these cases have in common that such practices simultaneously entail digital and non-digital contexts. As indicated earlier, lateral surveillance often involves physical/digital context collapse because many practices are rooted in online as well as offline contexts (Pagh, 2020). For instance, neighbours not only peek through their windows to see their neighbours entering and leaving their house, they also can check when they have received their messages in WhatsApp. Social surveillance in families takes place not only digitally via social media and location tracking or activity monitoring apps, but also in non-digital forms when parents simply check where their children are or what they are doing (by watching them or asking others to report on their children). Interestingly, when parents take their children's smartphones to unlock them and check their activities, interactions, and uses, their surveillance practices are simultaneously physical and digital. In essence, this research stresses that **lateral surveillance practices can only be adequately understood when collapsed contexts are taken into account.**

In line with the previous, my second theoretical contribution is also informed by context collapse and concerns privacy as contextual integrity. Privacy as contextual integrity (Nissenbaum, 2004, 2010, 2019) informed the selection of different contexts for studying privacy in this dissertation and also inspired the notion of contextualised surveillance practices. Some of my findings contribute to this theory because they illustrate how people negotiate the appropriateness of surveillance and privacy practices against a backdrop of collapsing contexts. **When physical and digital contexts collapse, information can be disseminated across digital and physical information flows, which complicates contextual integrity.** For instance, colleagues can simultaneously communicate via various digital channels that partly overlap with personal communication (like WhatsApp or social media) and also communicate face-to-face. Such multidimensional interactions challenge informational norms and complicate efforts to maintain transmission principles (aspects that constrain the flow of information). It is easier to construct and safeguard privacy expectations when work conversations are limited to email and face-to-face conversations than when they span across platforms and are mixed with personal conversation flows. My research shows that it becomes much more difficult to maintain informational norms when information flows are dispersed and cross-contextual. This concern will remain an issue to consider because recent Covid-19 lock-down situations have only amplified the dispersion and convergence of communication flows.

Third, the aforementioned conclusions touch upon the problematic lack of transparency of platform-based consumer surveillance that prevents users from controlling commercial data collection, processing, and sharing. While the empirical chapters not directly contribute to (critical) understandings of the functioning and consequences of platform ecosystems (Gillespie, 2010; Van Dijck et al., 2018; Zuboff, 2019), I provide insights into user experiences and perceptions of such ecosystems. This research shows how some users are mastering multi-tasking practices via many different (work) communication platforms. They negotiate between more commercially oriented platforms and open-source platforms that they deem more private and secure. The focus on sociomaterial aspects brings to light that user interfaces and particular settings are crucial and tangible elements of user practices. Also, Chapter 7 about household IPAs furthers an understanding of how concerns around platforms are related to tangible threats of security and surveillance. This not only adds to notions of privacy being multidimensional, but also indicates that platforms are only experienced when they become tangible through direct interactions, incidents, or by being addressed directly. For example, the household IPAs focus groups show that as soon as one person raises a tangible concern around platforms, others also start to reflect on the consequences of data collection by platforms. Current theoretical framing of platform ecosystems needs to be augmented by a focused account of mundane user experiences because **platforms can best be evaluated in relation to tangible devices and everyday user practices**.

Empirical lessons and reflections

The research in this dissertation can be characterised by its practice theory approach and a constructivist grounded theory set-up. In this section I reflect on my experiences as a researcher and present some empirical lessons. First, by following a constructivist grounded theory approach throughout this research (from the iterative interview guide design to intensive interviewing to a three-stage coding process, see chapter 2), I did not take the most time-efficient or straightforward route. The iterative nature of constructivist grounded theory and the fact that existing literature informs (instead of determines) the analysis, in practice meant that I had to move back and forth in the data analysis, and had to read many sources before, during, and after the analysis phase.

Semi-structured and intensive interviewing (characterised by open-ended and non-judgmental questions, Charmaz, 2014) enabled me to engage in many highly interesting conversations with the respondents. This formed an enriching experience for me personally because I learned so much from how people approach different situations and how they shared their personal doubts, concerns, and beliefs while talking through their everyday practices. More importantly, the open and interactive conversations also raised practices that I could have never anticipated, such as the reciprocal nature of location tracking in some families in Chapter 8. Moreover, if I had followed a more deductive analysis process, I am certain that many surprising findings would not have emerged from the interviews. By approaching the interview and focus group transcripts in a bottom-up manner via open coding, many new insights came to light – such as the *last seen* setting and *blue checks* as WhatsApp features that respondents actively used to manage absence and presence (Chapter 5).

In addition, the focus on sociomaterial practices provided opportunities to make latent processes and negotiations tangible that would have remained otherwise invisible. For example, by explaining how different phones can embody different information flows with different meanings in content, urgency, and nature (Chapter 6), intangible things like verbal conversations suddenly become palpable. And by asking respondents to discuss their practices, it often became clear that the purpose of particular activities (like WNCP practices aimed at safeguarding by assisting police efforts) divert from actual practices (citizens vigilantly guarding a neighbourhood, see Chapters 3 and 4). Furthermore, by analysing the meaning, or the purpose behind particular practices, I was able to indicate how similar practices can have different meanings for particular (groups of) people, e.g., safeguarding purposes entail different uses of WhatsApp than efforts to protect private time by limiting workplace communication. Respondents in different professional roles also provided different meanings of using social media (ranging from strictly personal interactions to self-employed professionals promoting their work online). In this research, a practice theory approach offered the means to establish a nuanced understanding of the multidimensional nature of everyday privacy and surveillance negotiations.

The temporal dimensions of this research provide insights into contextualised technology use over time. The fact that this research stretched over multiple years allows for some reflections. For instance, albeit unsurprising, social media use changed over time. During the first WNCP interviews in 2017, almost all respondents actively used Facebook. Shortly before the focus groups in Spring 2018, Cambridge Analytica's targeted political advertising via Facebook came to light (Tarran, 2018). This resulted in respondents being highly critical of Facebook. Yet, many respondents mentioned that they used Facebook regularly. In contrast, during the family interviews in 2021, most parents mentioned that they rarely used Facebook and if they were active on social media, they most often used Instagram. Their children named TikTok as their most used social media platform and were not active on Facebook. Additionally, household IPAs were not yet available at the time of the household IPA focus groups and only a few respondents used smart speakers. Three years later, the use of household IPAs seems domesticated in the family interviews. All respondents are aware of smart speakers and while only half of the families own such a device, the others mention friends and family that integrated smart speakers in their everyday lives. To sum up, all of these examples form indicators of the ever-changing nature of technology use, which reiterates that privacy and surveillance negotiations are dynamic. This needs to be considered when studying such practices by reflecting on how they are situated in a particular day and age.

Limitations of studying experiences

The limitations of the individual studies are indicated in the empirical chapters of this dissertation. In this section, I will briefly reflect on two overarching limitations of this largely qualitative research project. The first limitation is related to how I approached practice theory empirically. I analysed respondents' descriptions of practices, only sometimes supported by actual examples (like WNCP moderators showing me the group chats on their phone or children showing social media apps on their smartphones). As indicated in Chapter 2, I chose this approach to get a more rich and in-depth account of surveillance and privacy practices and experiences rather than asking respondents what they think about these concepts. However, ethnographic approaches (observing how people use technologies) might have revealed the discrepancies between descriptions of practices and actual behaviour better than my interviews did. Nevertheless, observing 100+ respondents in various contexts would not have been feasible within the scope of this project.

Furthermore, I conducted almost all the empirical research in this dissertation (with the exception of the 13 additional WNCP interviews in Chapter 4 and the quantitative analysis in Chapter 7). As indicated in Chapter 2, research findings are always influenced by the position of the researcher (Charmaz, 2014; Gherardi, 2017). This means that my research findings are, amongst others, influenced by my interdisciplinary education, social position, and cultural background. In order to allow for reflection and to provide insights into the decisions I made (for example by revealing and concealing certain elements), I aim to make the research process transparent by including methodological details and decisions in chapter 2, and the interview guides and codebooks in the appendices. Regardless of these measures, the results and conclusions presented in this dissertation are mainly based on my interpretations (informed by theory). Whereas this is the case for much qualitative research, this research might have led to (slightly) different conclusions if it was done by another researcher. Therefore, I invite others to do similar research in different settings, countries, or times to provide insights into how my findings transcend to additional contexts. Below I propose some contexts worthy to study.

Where to go from here? Suggestions for future research

This dissertation provides an in-depth account of the everyday practices of technology users. Parts of this research can be replicated to find connections between privacy and surveillance negotiations in different cultural, professional, and temporal contexts. Personally, I would love to dedicate more time to interviewing people in additional contexts to study their everyday experiences – following examples like Nippert-Eng's (2010) illuminating work on mundane privacy-preserving practices. However, the concerns I raised about (in)equality and transparency are also relevant in settings other than everyday user experiences.

Negotiations around appropriate contextualised surveillance practices not only occur in everyday domestic contexts but also play out on organisational and systematic levels. More so, my conclusions briefly address the underlying and overarching organisational, commercial, and systematic contexts connected to everyday practices. For instance, all everyday privacy and surveillance negotiations are in some way or form related to platform technologies. Researchers can inventory the everyday practices of professionals within platform companies to study issues around inequality and transparency in relation to privacy and surveillance negotiations. Studies can also focus on the practices of policy makers to study how they react to and regulate privacy and surveillance in relation to (in)equality and transparency.

Furthermore, smart homes and social media are increasingly organised via Artificial Intelligence. Apart from looking at the everyday practices of end users, a next step can be to examine the everyday practices of designers of AI. By studying how AI is constructed, practices around privacy and surveillance can be examined on the level of technology design. This way, efforts can be made to assure transparency, tangibility, and equality. Key to these suggested venues of research is to study privacy and surveillance in a contextualised and interconnected manner by taking practices on different levels into account. This dissertation provides insights into situated practices of technology users and presents detailed insights into how privacy and surveillance are experienced and negotiated in everyday life. Future research can follow this focused approach and add insights about different layers of practices to expand a detailed understanding of privacy and surveillance negotiations across different contexts.

References

Abdi, N., Ramokapane, K. M., & Such, J. M. (2019). *More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants*. Fifteenth Symposium on Usable Privacy and Security (SOUPS) 2019, Santa Clara, California, USA. https://www.usenix.org/conference/soups2019/presentation/abdi

Akkermans, M., & Vollaard, B. (2015). *Effect van het WhatsApp-project in Tilburg op het aantal woninginbraken – een evaluatie* [Effect of the WhatsApp project in Tilburg on the number of house break-ins – an evaluation]. Tilburg University. https://hetccv.nl/onderwerpen/woninginbraak/documenten/effect-van-het-whatsapp-project-in-tilburg-op-het-aantal-woninginbraken/

Akrich, M. (1992). The De-Scription of Technical Objects. In W. E. Bijker & J. Law (Eds.), *Shaping Technology / Building Society: Studies in sociotechnical change* (pp. 259–264). MIT Press. https://mitpress.mit.edu/books/shaping-technology-building-society

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3). https://firstmonday.org/ojs/index.php/fm/article/view/2142

Allmer, T. (2013). Critical Internet Privacy Studies. *Fast Capitalism*, *10*(1), 71–81. https://doi.org/10.32855/fcapital.201301.007

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Brooks Cole.

Andrejevic, M. (2002). The Work of Watching One Another: Lateral Surveillance, Risk, and Governance. *Surveillance & Society*, *2*(4), 479–497. https://doi-org.eur.idm.oclc.org/10.1080/ 07393180216561

Andrejevic, M. (2007). *Ispy: Surveillance and Power in the Interactive Era*. University Press of Kansas.

Atkinson, P., & Barker, R. (2020). 'Hey Alexa, what did I forget?': Networked devices, Internet search and the delegation of human memory. *Convergence*, *epub ahead of print*, 1–14. https://doi.org/10.1177/1354856520925740

Barnes, B. (2001). Practice as collective action. In T. R. Schatzki, K. Knorr Cetina, & E. von Savigny (Eds.), *The Practice Turn in Contemporary Theory* (pp. 25–36). Routledge.

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). https://doi.org/10.5210/fm.v11i9.1394

Bellair, P. E. (2000). Informal Surveillance and Street Crime: A Complex Relationship. *Criminology*, *38*(1), 137–170. https://doi.org/10.1111/j.1745-9125.2000.tb00886.x

Bennett, C. J., Haggerty, K. D., Lyon, D., & Steeves, V. (2014). *Transparent Lives: Surveillance in Canada*. Athabasca University Press.

Bervoets, E., Van Ham, T., & Ferwerda, H. (2016). *Samen signaleren: Burgerparticipatie bij sociale veiligheid* [Being alert together: Citizen participation in social security]. Platform 31. http://www.beke.nl/doc/2016/PL31-samen%20signaleren.pdf

Bittman, M., Brown, J. E., & Wajcman, J. (2009). The mobile phone, perpetual contact and time pressure. *Work, Employment and Society*, *23*(4), 673–691. https://doi.org/10.1177/0950017009344910

Boeije, H. (2002). A Purposeful Approach to the Constant Comparative Method in the Analysis of Quatlitative Interviews. *Quality & Quantity*, *36*, 391–409. https://doi-org.eur.idm.oclc.org/10.1023/A:1020909529486

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & de Vreese, C. H. (2018). Understanding the Effects of Personalization as a Privacy Calculus: Analyzing Self-Disclosure Across Health, News, and Commerce Contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Bol, N., Helberger, N., & Weert. (2018). Differences in mobile health app use: A source of new digital inequalities? *The Information Society*, *34*(3), 183-193. https://doi-org.eur.idm.oclc.org/10.1080/01972243.2018.1438550

Bowen, G. A. (2006). Grounded Theory and Sensitizing Concepts. *International Journal of Qualitative Methods*, *5*(3), 12–23. https://doi.org/10.1177/160940690600500304

Brause, S. R., & Blank, G. (2020). Externalized domestication: Smart speaker assistants, networks and domestication theory. *Information, Communication & Society*, *23*(5), 751–763. https://doi.org/10.1080/1369118X.2020.1713845

Brennen, B. S. (2013). *Qualitative Research Methods for Media Studies*. Routledge.

Brisson-Boivin, K. (2018). *The Digital Well-Being of Canadian Families*. MediaSmarts. https://mediasmarts.ca/sites/default/files/publication-report/full/digital-canadian-families.pdf

Brown, B. (2001). *Studying the internet experience* (HP Laboratories Technical Report HPL-2001-49; p. 24). http://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf

Bucher, T., & Helmond, A. (2017). The affordances of social media platforms. In J. Burgess, T. Poell, & A. Marwick (Eds.), *The SAGE handbook of social media* (pp. 233–253). SAGE.

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., & Viljoen, S. (2020). The chilling effects of algorithmic profiling: Mapping the issues. *Computer Law & Security Review*, *36*, 1–15. https://doi.org/10.1016/j.clsr.2019.105367

Burchell, K. (2015). Tasking the everyday: Where mobile and online communication take time. *Mobile Media & Communication*, *3*(1), 36–52. https://doi.org/10.1177/2050157914546711

Burchell, K. (2017). Finding Time for Goffman: When absence is more telling than presence. In T. Markham & S. Rodgers (Eds.), *Conditions of mediation: Phenomenological perspectives on media* (pp. 185–196). Peter Lang.

Çankaya, S. (2015). De politiële surveillance van ras en etniciteit [The Police Surveillance of Race and Ethnicity]. *Cahiers Politiestudies*, *6*(35), 13–33.

Carstensen, T. (2015). The Internet as Material Object in Social Practices: Recording and Analysis of Human-Internet Interactions. *Nature + Culture; New York*, *10*(3), 284–302. http://dx.doi.org.eur.idm.oclc.org/10.3167/nc.2015.100303

Chan, J. (2008). The New Lateral Surveillance and a Culture of Suspicion. In M. Deflem (Ed.), *Surveillance and Governance: Crime Control and Beyond* (pp. 223–240). Emerald.

Chandrasekaran, V., Fawaz, K., Mutlu, B., & Banerjee, S. (2018). Characterizing Privacy Perceptions of VoiceAssistants: A Technology Probe Study. *ArXiv Preprint*. https://deepai.org/publication/characterizing-privacy-perceptions-of-voice-assistants-a-technology-probe-study

Chang, L., & Mogg, T. (2018, March 8). Amazon offers a reason for Alexa's 'random,' creepy laugh. *Digital Trends*. https://www.digitaltrends.com/home/amazon-alexa-laugh/

Charmaz, K. (2014). *Constructing Grounded Theory* (2nd ed.). SAGE.

Check In & Panic: Keep Your Family Safe and in Sync! (2012, March 8). *Life360*. https://www.life360.com/blog/check-in-panic-keep-your-family-safe-and-in-sync/

Child, J. T., Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior*, *28*(5), 1859–1872. https://doi.org/10.1016/j.chb.2012.05.004

Cho, E. (2019). Hey Google, Can I Ask You Something in Private? *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–9. https://doi.org/10.1145/3290605.3300488

Christensen, T. H., & Røpke, I. (2010). Can practice theory inspire studies of ICTs in everyday life. In B. Bräuchler & J. Postill (Eds.), *Theorising media and practice* (pp. 233–256). Berghahn books.

Christl, W. (2017). *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions*. Cracked Labs. https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Church, K., & de Oliveira, R. (2013). What's Up with Whatsapp?: Comparing Mobile Instant Messaging Behaviors with Traditional SMS. *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services*, 352–361. https://doi.org/10.1145/2493190.2493225

Ciborra, C. U. (1992). From thinking to tinkering: The grassroots of strategic information systems. *The Information Society*, *8*(4), 297–309. https://doi.org/10.1080/01972243.1992.9960124

Cino, D., Mascheroni, G., & Wartella, E. (2020). "The Kids Hate It, but We Love It!": Parents' Reviews of Circle. *Media and Communication*, *8*(4), 208–217. https://doi.org/10.17645/mac.v8i4.3247

Clark, S. C. (2000). Work/Family Border Theory: A New Theory of Work/Family Balance. *Human Relations*, *53*(6), 747–770. https://doi.org/10.1177/0018726700536001

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, *13*(1), 3–21. https://doi.org/10.1007/BF00988593

Coyne, I. T. (1997). Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries? *Journal of Advanced Nursing*, *26*(3), 623–630. https://doi.org/10.1046/j.1365-2648.1997.t01-25-00999.x

Creepy: Amazon-speakers lachen je onverwacht uit [Creepy: Amazon-speakers laugh unexpectedly]. (2018, March 8). *RTL Nieuws*. https://www.rtlnieuws.nl/tech/artikel/3914526/creepy-amazon-speakers-lachen-je-onverwacht-uit

Crouter, A. C., & Head, M. R. (2002). Parental Monitoring and Knowledge of Children. In M. H. Bornstein (Ed.), *Handbook of Parenting: Being and becoming a parent* (pp. 461–483). Psychology Press.

DDMA. (2021). *How the Dutch think about data and privacy* (DDMA Privacy monitor 2021). Data Driven Marketing Association Data Driven Marketing Association. https://ddma.nl/privacy-monitor/

De Leyn, T., Waeterloos, C., Wolf, R. D., Vanhaelewyn, B., Ponnet, K., & Marez, L. D. (2021). Teenagers' reflections on media literacy initiatives at school and everyday media literacy discourses. *Journal of Children and Media*, *Epub ahead of print*, 1–19. https://doi.org/10.1080/17482798.2021.1952463

De Reuver, M., Nikou, S., & Bouwman, H. (2016). Domestication of smartphones and mobile applications: A quantitative mixed-method study. *Mobile Media & Communication*, *4*(3), 347–370. https://doi.org/10.1177/2050157916649989

De Vries, A. (2016, February 1). BuurtWhatsApp: Goed beheer is complex. *Social Media DNA*. http://socialmediadna.nl/buurtwhatsapp-goed-beheer-is-complex/

De Wolf, R., Willaert, K., & Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior*, *35*, 444–454. https://doi.org/10.1016/j.chb.2014.03.010

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *7*(1), 61–80. https://www.jstor.org/stable/23015781

Duxbury, L., Higgins, C., Smart, R., & Stevenson, M. (2014). Mobile Technology and Boundary Permeability. *British Journal of Management*, *25*(3), 570–588. https://doi.org/10.1111/1467-8551.12027

Ervasti, M., Laitakari, J., & Hillukkala, M. (2016). 'I want to know where my child is at all times' – field study of a location-aware safety service for schoolchildren. *Behaviour & Information Technology*, *35*(10), 833–852. https://doi.org/10.1080/0144929X.2016.1201144

Esmeijer, L., & Luning, M. (1978). Surinamers in de ogen van de Amsterdamse politie. In F. Bovenkerk (Ed.), *Omdat zij anders zijn: Patronen van rasdiscriminatie in Nederland* (pp. 136–165). Boom Koninklijke Uitgevers.

Esmonde, K. (2020). 'There's only so much data you can handle in your life': Accommodating and resisting self-surveillance in women's running and fitness tracking practices. *Qualitative Research in Sport, Exercise and Health*, *12*(1), 76–90. https://doi.org/10.1080/2159676X.2019.1617188

Evans, S. K., Pearce, K. E., Vitak, J., & Treem, J. W. (2017). Explicating Affordances: A Conceptual Framework for Understanding Affordances in Communication Research. *Journal of Computer-Mediated Communication*, *22*(1), 35–52. https://doi.org/10.1111/jcc4.12180

Fiesler, C., Dye, M., Feuston, J. L., Hiruncharoenvate, C., Hutto, C. J., Morrison, S., Khanipour Roshan, P., Pavalanathan, U., Bruckman, A. S., De Choudhury, M., & Gilbert, E. (2017). What (or Who) Is Public?: Privacy Settings and Social Media Content Sharing. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 567–580. https://doi.org/10.1145/2998181.2998223

Frampton, B. D., & Child, J. T. (2013). Friend or not to friend: Coworker Facebook friend requests as an application of communication privacy management theory. *Computers in Human Behavior*, *29*(6), 2257–2264. https://doi.org/10.1016/j.chb.2013.05.006

Fuchs, C. (2012). The Political Economy of Privacy on Facebook. *Television & New Media*, *13*(2), 139–159. https://doi.org/10.1177/1527476411415699

Furey, E., & Blue, J. (2018). She Knows Too Much – Voice Command Devices and Privacy. *2018 29th Irish Signals and Systems Conference (ISSC)*, 1–6. https://doi.org/10.1109/ISSC.2018.8585380

Fussel, S. (2020, August 23). Meet the Star Witness: Your Smart Speaker. *Wired*. https://www.wired.com/story/star-witness-your-smart-speaker/

Geeng, C., & Roesner, F. (2019). Who's In Control? Interactions In Multi-User Smart Homes. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3290605.3300498

Gherardi, S. (2017). Sociomateriality, posthuman practice theory. In A. Hui, S. Schatzki Theodore, & E. Shove (Eds.), *The nexus of practices: Connections, constellations, practitioners*. Routledge.

Gibson, J., J. (2014). The Theory of Affordances (1979). In J. J. Gieseking, W. Mangold, C. Katz, S. Low, & S. Saegert (Eds.), *The People, Place, and Space Reader* (pp. 56–60). Routledge.

Gillespie, T. (2010). The politics of ‘platforms’. *New Media & Society*, *12*(3), 347–364. https://doi.org/10.1177/1461444809342738

Glaser, B. G., & Strauss, A. L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Transaction. http://www.transactionpub.com/title/978-0-202-30260-7.html

Haggerty, K. D. (2012). Surveillance, crime and the police. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge Handbook of Suveillance Studies* (pp. 235–243). Routledge.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605–622. https://doi.org/10.1080 / 0007131002001528 0

Hampton, K. N. (2007). Neighborhoods in the Network Society the e-Neighbors study. *Information, Communication & Society*, *10*(5), 714–748. https://doi.org/10.1080/13691180701658061

Hargittai, E., & Hsieh, Y. P. (2012). Succinct survey measures of web-use skills. *Social Science Computer Review*, *30*(1), 95–107. https://doi.org/10.1177/0894439310397146

Henderson, A. C., Harmon, S. M., & Houser, J. (2010). A New State of Surveillance? Applying Michel Foucault to Modern Motherhood. *Surveillance & Society*, *7*(3/4), 231–247. https://doi.org/10.24908/ss.v7i3/4.4153

Horcher, G. (2018, May 25). Woman says her Amazon device recorded private conversation, sent it out to random contact. *KIRO7*. https://www.kiro7.com/news/local/woman-says-her-amazon-device-recorded-private-conversation-sent-it-out-to-random-contact/755507974

Horst, H. V. D., & Messing, J. (2006). “It’s Not Dutch to Close the Curtains”. *Home Cultures*, *3*(1), 21–37. https://doi.org/10.2752/174063106778053264

Howard-Payne, L. (2016). Glaser or Strauss? Considerations for selecting a grounded theory study. *South African Journal of Psychology*, *46*(1), 50–62. https://doi.org/10.1177/0081246315593071

Huang, Y., Obada-Obieh, B., & Beznosov, K. (Kosta). (2020). Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. http://doi.org/10.1145/3313831.3376529

Hughes, K. (2015). The social value of privacy, the value of privacy to society and human rights discourse. In B. Roessler & D. Mokrosinska (Eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (pp. 225–243). Cambridge University Press.

Huisregels [House rules]. (2015, July 9). *WhatsApp Buurtpreventie*. https://wabp.nl/huisregels/

Humphreys, L., Karnowski, V., & Pape, T. von. (2018). Smartphones as Metamedia: A Framework for Identifying the Niches Structuring Smartphone Use. *International Journal of Communication*, *12*, 2793–2809.

Jahn, K., Klesel, M., Lemmer, K., Weigel, A., & Niehaves, B. (2016). Individual Boundary Management: An Empirical Investigation on Technology-related Tactics. *PACIS 2016 Proceedings*, 268–271. https://aisel.aisnet.org/pacis2016/268

Kantar. (2019). *The General Data Protection Regulation* (Special Eurobarometer No. 487). Kantar. https://privacy-web.nl/wp-content/uploads/po_assets/560173.pdf

Karapanos, E., Teixeira, P., & Gouveia, R. (2016). Need fulfillment and experiences on social media: A case on Facebook and WhatsApp. *Computers in Human Behavior*, *55*, 888–897. https://doi.org/10.1016/j.chb.2015.10.015

Katz, C. (2001). The State Goes Home: Local Hyper-Vigilance of Children and the Global Retreat from Social Reproduction. *Social Justice*, *28*(3), 47–56. https://www.jstor.org/stable/29768093

Kerr, M., Stattin, H., & Burk, W. J. (2010). A Reinterpretation of Parental Monitoring in Longitudinal Perspective. *Journal of Research on Adolescence*, *20*(1), 39–64. https://doi.org/10.1111/j.1532-7795.2009.00623.x

Kinsella, B. (2020, April 28). Amazon Smart Speaker Market Share Falls to 53% in 2019 with Google The Biggest Beneficiary Rising to 31%, Sonos Also Moves Up. *Voicebot.Ai*. https://voicebot.ai/2020/04/28/amazon-smart-speaker-market-share-falls-to-53-in-2019-with-google-the-biggest-beneficiary-rising-to-31-sonos-also-moves-up/

Kinsella, B., & Mutchler, A. (2019). *Smart Speaker Consumer Adoption Report March 2019 U.S.* Voiebot.ai. https://voicebot.ai/wp-content/uploads/2019/03/smart_speaker_consumer_adoption_report_2019.pdf

Kitzinger, J., & Barbour, R., S. (1999). Introduction: The challenge and promise of focus groups. In J. Kitzinger & R. Barbour S. (Eds.), *Developing Focus Group Research* (pp. 1–21). SAGE Publications.

Könings, B., Schaub, F., Weber, M., & Kargl, F. (2010). *Towards territorial privacy in smart environments*. AAAI 2010 Spring Symposium. https://doi.org/10.18725/OPARU-1727

Koops, B.-J. (2018). Privacy Spaces. *West Virginia Law Review*, *121*(2), 612–665. https://heinonline.org/HOL/P?h=hein.journals/wvb121&i=629

Koops, B.-J., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T., & Galic, M. (2016). A Typology of Privacy. *University of Pennsylvania Journal of International Law*, *38*(2), 483–576. https://heinonline.org/HOL/P?h=hein.journals/upjiel38&i=489

Krouse, S. S., & Afifi, T. D. (2007). Family-to-work Spillover Stress: Coping Communicatively in the Workplace. *Journal of Family Communication*, *7*(2), 85–122. https://doi.org/10.1080/15267430701221537

Kurz, D. (2009). "I Trust Them but I Don't Trust Them" Issues and Dilemmas in Monitoring Teenagers. In M. K. Nelson & A. I. Garey (Eds.), *Who's Watching?: Daily Practices of Surveillance among Contemporary Families* (pp. 260–276). Vanderbilt University Press.

Laitinen, K., & Sivunen, A. (2020). Enablers of and constraints on employees' information sharing on enterprise social media. *Information Technology & People*, *34*(2), 642–665. https://doi.org/10.1108/ITP-04-2019-0186

Larsen, M., & Piché, J. (2010). Public Vigilance Campaigns and Participatory Surveillance after 11 September 2001. In S. P. Hier & J. Greenberg (Eds.), *Surveillance: Power, Problems, and Politics* (pp. 187–202). UBC Press.

Larsson, S. (2017). A First Line of Defence? Vigilant Surveillance, Participatory Policing, and the Reporting of 'Suspicious' Activity. *Surveillance & Society*, *15*(1), 94–107. https://doi.org/10.24908/ss.v15i1.5342

Latour, B. (1992). Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts. In W. E. Bijker & J. Law (Eds.), *Shaping Technology / Building Society: Studies in sociotechnical change* (pp. 225–258). MIT Press.

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1–31. https://doi.org/10.1145/3274371

Leaver, T. (2015). Born Digital?: Presence, Privacy, and Intimate Surveillance. In J. Hartley & W. Qu (Eds.), *Re-Orientation: Translingual Transcultural Transmedia. Studies in narrative, language, identity, and knowledge* (pp. 149–160). Fudan University Press.

Leaver, T. (2017). Intimate Surveillance: Normalizing Parental Monitoring and Mediation of Infants Online. *Social Media + Society*, *3*(2), 1–10. https://doi.org/10.1177/2056305117707192

Lee, E. W. J., Ho, S. S., & Lwin, M. O. (2017). Explicating problematic social network sites use: A review. *New Media & Society*, *19*(2), 308–326. https://doi.org/10.1177/1461444816671891

Leerling & ouder: Magister Web en Magister App [Student & parent: Magister Web and Magister App]. (n.d.). *Magister*. Retrieved 26 July 2021, from https://www.magister.nl/leerling-ouder/

Lei, X., Tu, G.-H., Liu, A. X., Li, C.-Y., & Xie, T. (2017). The Insecurity of Home Digital Voice Assistants—Amazon Alexa as a Case Study. *ArXix Preprint*. http://arxiv.org/abs/1712.03327

Liao, Y., Vitak, J., Kumar, P., Zimmer, M., & Kritikos, K. (2019). Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption. *Information in Contemporary Society. IConference 2019.* 102–113. https://doi.org/10.1007/978-3-030-15742-5_9

Licoppe, C. (2004). 'Connected' Presence: The Emergence of a New Repertoire for Managing Social Relationships in a Changing Communication Technoscape. *Environment and Planning D: Society and Space*, *22*(1), 135–156. https://doi.org/10.1068/d323t

Licoppe, C. (2010). The "Crisis of the Summons": A Transformation in the Pragmatics of "Notifications," from Phone Rings to Instant Messaging. *The Information Society*, *26*(4), 288–302. https://doi.org/10.1080/01972243.2010.489859

Livingstone, S. (2004). Media Literacy and the Challenge of New Information and Communication Technologies. *The Communication Review*, *7*(1), 3–14. https://doi.org/10.1080/10714420490280152

Livingstone, S., & Blum-Ross, A. (2020). *Parenting for a Digital Future: How Hopes and Fears about Technology Shape Children's Lives* (1st edition). Oxford University Press.

Livingstone, S., Mascheroni, G., Dreier, M., Chaudron, S., & Lagae, K. (2015). *How parents of young children manage digital devices at home: The role of income, education and parental style*. EU Kids Online. http://eprints.lse.ac.uk/63378/

Livingstone, S., Mascheroni, G., & Staksrud, E. (2015). *Developing a framework for researching children's online risks and opportunities in Europe*. EU Kids Online. http://eprints.lse.ac.uk/63378/

Lub, V. (2018). *Neighbourhood Watch in a Digital Age: Between Crime Control and Culture of Control*. Springer International Publishing. https://doi.org/10.1007/978-3-319-67747-7

Lub, V., & De Leeuw, T. (2017). Perceptions of Neighbourhood Safety and Policy Response: A Qualitative Approach. *European Journal on Criminal Policy and Research*, *23*(3), 425–440. https://doi-org.eur.idm.oclc.org/10.1007/s10610-016-9331-0

Lub, V., & De Leeuw, T. (2019). *Politie en actief burgerschap: Een veilig verbond? Een onderzoek naar samenwerking, controle en (neven)effecten [Police and active citizenship: A secure alliance? A study into collaboration, control and (side) effects]* (No. 108). Politie & Wetenschap. https://www.politieenwetenschap.nl/publicatie/politiewetenschap/2019/politie-en-actief-burgerschap-een-veilig-verbond-322/

Lutz, C., & Newlands, G. (2021). Privacy and smart speakers: A multi-dimensional approach. *The Information Society*, *37*(2), 147–162. https://doi.org/10.1080/01972243.2021.1897914

Lyon, D. (2007). *Surveillance studies: An overview*. Polity press

Lyon, D. (2018). *The Culture of Surveillance: Watching As a Way of Life*. Polity press

Magsamen-Conrad, K., Checton, M. G., & Venetis, M. K. (2013). Privacy and disclosure at work: The implications of self-concealment and anonymity. *Proceedings of the 2nd Annual International Conference on Journalism & Mass Communications*, 118–126. https://doi.org/10.1037/e639892013-018

Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., & Wagner, D. (2019). Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies*, *2019*(4), 250–271. https://doi.org/10.2478/popets-2019-0068

Manikonda, L., Deotale, A., & Kambhampati, S. (2017). What's up with Privacy?: User Preferences and Privacy Concerns in Intelligent Personal Assistants. *ArXiv Preprint*. http://arxiv.org/abs/1711.07543

Mann, S. (2016). Surveillance (Oversight), Sousveillance (Undersight), and Metaveillance (Seeing Sight Itself). *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 1–10. http://www.cv-foundation.org/openaccess/content_cvpr_2016_workshops/w29/html/Mann_Surveillance_Oversight_Sousveillance_CVPR_2016_paper.html

Mannell, K. (2019). A typology of mobile messaging's disconnective affordances. *Mobile Media & Communication*, *7*(1), 76–93. https://doi.org/10.1177/2050157918772864

Manokha, I. (2018). Surveillance, Panopticism, and Self-Discipline in the Digital Age. *Surveillance & Society*, *16*(2), 219–237. https://doi.org/10.24908/ss.v16i2.8346

Marsh, A., Downs, J., & Cranor, L. (2017). *Experts' Views on Digital Parenting Strategies (CMU-CyLab-17-002)*. https://doi.org/10.1184/R1/6467891.v1

Marwick, A. (2012). The Public Domain: Surveillance in Everyday Life. *Surveillance & Society*, *9*(4), 378–393. https://doi.org/10.24908/ss.v9i4.4342

Marwick, A., & boyd, danah. (2010). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133. https://doi-org.eur.idm.oclc.org/10.1177/1461444810365313

Marx, G., & Steeves, V. (2010). From the Beginning: Children as Subjects and Agents of Surveillance. *Surveillance & Society*, *7*(3/4), 192–230. https://doi.org/10.24908/ss.v7i3/4.4152

Marx, G. T. (2015a). Surveillance Studies. In J. D. Wright (Ed.), *International Encyclopedia of the Social & Behavioral Sciences* (pp. 733–741). Elsevier. https://doi.org/10.1016/B978-0-08-097086-8.64025-4

Marx, G. T. (2015b). Coming to terms: The kaleidoscope of privacy and surveillance. In B. Roessler & D. Mokrosinska (Eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (pp. 32–49). Cambridge University Press.

Marx, G. T., & Steeves, V. (2010). From the Beginning: Children as Subjects and Agents of Surveillance. *Surveillance & Society*, *7*(3/4), 192–230. https://doi.org/10.24908/ss.v7i3/4.4152

Mascheroni, G., & Vincent, J. (2016). Perpetual contact as a communicative affordance: Opportunities, constraints, and emotions. *Mobile Media & Communication*, *4*(3), 310–326. https://doi.org/10.1177/2050157916639347

Mazmanian, M., & Lanette, S. (2017). 'Okay, One More Episode': An Ethnography of Parenting in the Digital Age. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 2273–2286. https://doi.org/10.1145/2998181.2998218

McLean, G., & Osei-Frimpong, K. (2019). Hey Alexa. Examine the variables influencing the use of artificial intelligent in-home voice assistants. *Computers in Human Behavior*, *99*, 28–37. https://doi.org/10.1016/j.chb.2019.05.009

McNair, C. (2019, January 2). Global Smart Speaker Users 2019 [Insider Intelligence]. *EMarketer*. https://www.emarketer.com/content/global-smart-speaker-users-2019

Mehlbaum, S. L., & Steden, R. van. (2018). *Doe-het-zelf surveillance: Een onderzoek naar de werking en effecten van WhatsApp-buurtgroepen [Do-it-yourself surveillance: An investigation into the functioning and effects of WhatsApp neighborhood groups]*. SDU. https://research.vu.nl/en/publications/doe-het-zelf-surveillance-een-onderzoek-naar-de-werking-en-effect

Merchant, G. (2012). Mobile practices in everyday life: Popular digital technologies and schooling revisited. *British Journal of Educational Technology*, *43*(5), 770–782. https://doi.org/10.1111/j.1467-8535.2012.01352.x

Mols, A., & Janssen, S. (2017). Not Interesting Enough to be Followed by the NSA. *Digital Journalism*, *5*(3), 277–298. https://doi.org/10.1080/21670811.2016.1234938

Morgan, D. (1997). *Focus Groups as Qualitative Research*. SAGE Publications.

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society*, *374*(2083), 20160118. https://doi.org/10.1098/rsta.2016.0118

Nagy, P., & Neff, G. (2015). Imagined Affordance: Reconstructing a Keyword for Communication Theory. *Social Media + Society*, *1*(2), 1–9. https://doi.org/10.1177/2056305115603385

Nelson, M. K., & Garey, A. I. (2009). *Who's Watching?: Daily Practices of Surveillance among Contemporary Families*. Vanderbilt University Press. https://doi.org/10.2307/j.ctv17vf76w

Nextdoor Public Agency. (n.d.). *Nextdoor.Com*. Retrieved 10 August 2021, from https://go.us.nextdoor.com/agency

Niculescu Dinca, V. (2016). *Policing Matter(s)* [Maastricht University]. https://cris.maastrichtuniversity.nl/portal/en/publications/policing-matters(b-911f31c-f8e8-44e9-999c-5c8edcafd7b7).html

Nikken, P. (2021). *Monitor Mediagebruik kinderen 7-12 jaar [Monitor Media use children 7-12]*. Netwerk Mediawijsheid. https://www.mediawijzer.net/kennisbank/monitor-mediagebruik-kinderen-7-12-jaar/

Nippert-Eng, C. E. (1996a). *Home and Work: Negotiating Boundaries Through Everyday Life*. University of Chicago Press.

Nippert-Eng, C. E. (1996b). Calendars and keys: The classification of "home" and "work". *Sociological Forum*, *11*(3), 563–582. https://doi.org/10.1007/BF02408393

Nippert-Eng, C. E. (2010). Islands of Privacy. In *Islands of Privacy*. University of Chicago Press.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*, 119–157. http://www.kentlaw.edu/faculty/rwarner/classes/internetlaw/2011/materials/nissenbaum_norms.pdf

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Nissenbaum, H. (2019). Contextual Integrity Up and Down the Data Food Chain. *Theoretical Inquiries in Law*, *20*(1), 221–256. http://www7.tau.ac.il/ojs/index.php/til/article/view/1614

Olson-Buchanan, J. B., & Boswell, W. R. (2006). Blurring boundaries: Correlates of integration and segmentation between work and nonwork. *Journal of Vocational Behavior*, *68*(3), 432–445. https://doi.org/10.1016/j.jvb.2005.10.006

Opree, S., Stam, B., & Jansz, J. (2021). *Mediawijsheid onderzoek onder de loep: De staat van het onderzoek naar mediawijsheid in Nederland (2013t/m 2020) [Media literacy research under the microscope: The state of media literacy research in the Netherlands (2013-2020)]* [Rapport in opdracht van Ministerie van Onderwijs, Cultuur en Wetenschap]. Erasmus Research Center for Media, Communication and Culture. https://www.eur.nl/en/eshcc/media/2021-02-eindrapport-mediawijsheid-22-01-2021

Orlikowski, W. J. (2007). Sociomaterial Practices: Exploring Technology at Work. *Organization Studies*, *28*(9), 1435–1448. https://doi.org/10.1177/0170840607081138

Pagh, J. (2020). Managing Context Collapses: The Internet as a Conditioning Technology in the Organization of Practices. *International Journal of Communication*, *12*, 2810–2827. https://ijoc.org/index.php/ijoc/article/view/11872

Park, Y. J., & Mo Jang, S. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, *38*, 296–303. https://doi.org/10.1016/j.chb.2014.05.041

Patton, M. Q. (1990). *Qualitative evaluation and research methods* (2nd ed.). SAGE.

Peek of the Net. (2017, February 4). *Google Home Official Ad*. https://www.youtube.com/watch?v=OsXedJq1aWE&t=2s

Perez, S. (2019, February 5). Report: Smart speaker adoption in US reaches 66M units, with Amazon leading. *TechCrunch*. http://social.techcrunch.com/2019/02/05/report-smart-speaker-adoption-in-u-s-reaches-66m-units-with-amazon-leading/

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. SUNY Press. http://www.sunypress.edu/p-3659-boundaries-of-privacy.aspx

Petronio, S. (2010). Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation? *Journal of Family Theory & Review*, *2*(3), 175–196. https://doi.org/10.1111/j.1756-2589.2010.00052.x

Petronio, S. (2012). *Boundaries of Privacy: Dialectics of Disclosure*. State University of New York Press.

Petronio, S., & Caughlin, J. P. (2005). Communication Privacy Management Theory: Understanding Families. In D. Braithwaite & L. Baxter (Eds.), *Engaging Theories in Family Communication: Multiple Perspectives* (pp. 35–49). Sage.

Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: Utility of communication privacy management theory. *Current Opinion in Psychology*, *31*, 76–82. https://doi.org/10.1016/j.copsyc.2019.08.009

Pielot, M., de Oliveira, R., Kwak, H., & Oliver, N. (2014). Didn't You See My Message? Predicting Attentiveness to Mobile Instant Messages. *CHI '14 Toronto, Canada*, 3319–3328. https://doi-org.eur.idm.oclc.org/10.1145/2556288.2556973

PII-Filter voor onnodige persoonlijke informatie [PII-Filter for unneccessary personal information] (n.d.). SIDN fonds. Retrieved 16 August 2021, from https://www.sidnfonds.nl/nieuws/filter-voor-onnodige-persoonlijke-informatie

Politietaken [Police tasks]. (n.d.). *Politie*. Retrieved 12 January 2018, from https://www.politie.nl/themas/politietaken.html

Press Kit: Neighbors and Neighbors Public Safety Service. (n.d.). *Ring Help*. Retrieved 10 August 2021, from https://support.ring.com/hc/en-us/articles/360051706931-Press-Kit-Neighbors-and-Neighbors-Public-Safety

Pridmore, J. (2012). Consumer surveillance: Context, perspectives and concerns in the personal information economy. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge Handbook of Suveillance Studies* (pp. 231–329). Routledge.

Pridmore, J., & Mols, A. (2020). Personal choices and situated data: Privacy negotiations and the acceptance of household Intelligent Personal Assistants. *Big Data & Society, 7*(1), 2053951719891748. https://doi.org/10.1177/2053951719891748

Pridmore, J., Mols, A., Wang, Y., & Holleman, F. (2018). Keeping an eye on the neighbours: Police, citizens, and communication within mobile neighbourhood crime prevention groups. *The Police Journal: Theory, Practice and Principles*, *92*(2), 97–120. https://doi.org/10.1177/0032258X18768397

Pridmore, J., Zimmer, M., Vitak, J., Mols, A., Trottier, D., Kumar, P. C., & Liao, Y. (2019). Intelligent Personal Assistants and the Intercultural Negotiations of Dataveillance in Platformed Households. *Surveillance & Society*, *17*(1/2), 125–131. https://doi.org/10.24908/ss.v17i1/2.12936

Pridmore, J., & Zwick, D. (2011). Editorial—Marketing and the Rise of Commercial Consumer Surveillance. *Surveillance & Society*, *8*(3), 269–277. https://doi.org/10.24908/ss.v8i3.4163

Purenne, A., & Palierse, G. (2016). Towards Cities of Informers? Community-Based Surveillance in France and Canada. *Surveillance & Society*, *15*(1), 79–93. https://doi.org/10.24908/ss.v15i1.5619

Rastogi, N., & Hendler, J. (2017). WhatsApp Security and Role of Metadata in Preserving Privacy. *Proceedings of the 12th International Conference on Cyber Warfare and Security*, 269–274. https://arxiv.org/abs/1701.06817

Reckwitz, A. (2002). Toward a Theory of Social Practices. *European Journal of Social Theory*, *5*(2), 243–263. https://doi.org/10.1177/13684310222225432

Reeves, J. (2012). If You See Something, Say Something: Lateral Surveillance and the Uses of Responsibility. *Surveillance & Society*, *10*(3/4), 235–248. https://doi.org/10.24908/ss.v10i3/4.4209

Regan, P. M. (2015). Privacy and the common good: Revisited. In B. Roessler & D. Mokrosinska (Eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (pp. 50–70). Cambridge University Press.

Rooney, T. (2010). Trusting Children: How do surveillance technologies alter a child's experience of trust, risk and responsibility? *Surveillance & Society*, *7*(3/4), 344–355. https://doi.org/10.24908/ss.v7i3/4.4160

Rose, N. (1996). Governing “advanced” liberal democracies. In A. Barry & N. Rose (Eds.), *Foucault and Political Reason: Liberalism, Neo-Liberalism, and Rationalities of Government* (pp. 37–64). University of Chicago Press.

Russakovskii, A. (2017, October 10). Google is permanently nerfing all Home Minis because mine spied on everything I said 24/7. *Android Police*. https://www.androidpolice.com/2017/10/10/google-nerfing-home-minis-mine-spied-everything-said-247/

Ryan, B. J. (2008). Northern Ireland’s District Policing Partnerships and the Participatory Ideals. *Irish Political Studies*, *23*(3), 341–361. https://doi.org/10.1080/07907180802246677

Sandhu, A., & Haggerty, K. D. (2015). Private eyes: Private policing and surveillance. In R. Abrahamsen & A. Leander (Eds.), *Routledge Handbook of Private Security Studies*. Routledge.

Sayah, S. (2013). Managing work–life boundaries with information and communication technologies: The case of independent contractors. *New Technology, Work and Employment*, *28*(3), 179–196. https://doi.org/10.1111/ntwe.12016

Schalow, P. R., Winkler, T. J., Repschlaeger, J., & Zarnekow, R. (2013). The blurring boundaries of work-related and personal media use. *Proceedings of the 21st European Conference on Information Systems*, 1–12. https://aisel.aisnet.org/ecis2013_cr/212/

Schatzki, T. R. (2002). *The site of the social: A philosophical account of the constitution of social life and change*. Pennsylvania State University Press

Schatzki, T. R. (2005). Introduction: Practice theory. In T. R. Schatzki, K. Knorr Cetina, & E. von Savigny (Eds.), *The Practice Turn in Contemporary Theory* (pp. 10–23). Routledge

Schoeman, F. (1984). Privacy: Philosophical Dimensions. *American Philosophical Quarterly*, *21*(3), 199–213. https://www.jstor.org/stable/20014049

Seufert, M., Hosfeld, T., Schwind, A., Burger, V., & Tran-Gia, P. (2016). Group-based communication in WhatsApp. *2016 IFIP Networking Conference*, 536–541. https://doi.org/10.1109/IFIPNetworking.2016.7497256

Shearing, C. (1994). Participatory Policing: Modalities in Lay Participation. *Imbizo*, *1*(2), 5–10. https://papers.ssrn.com/abstract=2832112

Shirazi, A. S., Henze, N., Dingler, T., Pielot, M., Weber, D., & Schmidt, A. (2014). Large-scale assessment of mobile notifications. In *CHI ’14 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3055–3064). ACM. https://dl.acm.org/citation.cfm?id=2557189

Shove, E., Pantzar, M., & Watson, M. (2012). *The Dynamics of Social Practice: Everyday Life and how it Changes*. SAGE.

Siegert, S., & Löwstedt, J. (2019). Online boundary work tactics: An affordance perspective. *New Technology, Work and Employment*, *34*(1), 18–36. https://doi.org/10.1111/ntwe.12126

Simmons, H. (2020). Feeling Judged: Parenting Culture and Interpersonal Surveillance. In H. Simmons (Ed.), *Surveillance of Modern Motherhood: Experiences of Universal Parenting Courses* (pp. 93–118). Springer International Publishing. https://doi.org/10.1007/978-3-030-45363-3_5

Simpson, B. (2014). Tracking children, constructing fear: GPS and the manufacture of family safety. *Information & Communications Technology Law*, *23*(3), 273–285. https://doi.org/10.1080/13600834.2014.970377

Slimme speaker verovert huiskamer consument [Smart speaker conquers consumer's living room]. (2020, April 30). *Multiscope*. http://www.multiscope.nl/persberichten/slimme-speaker-verovert-huiskamer-consument/

Slimme speakers in half miljoen huishoudens [Smart speakers in half a million households]. (2019, May 19). *Multiscope*. http://www.multiscope.nl/persberichten/slimme-speakers-in-half-miljoen-huishoudens.html

Smeets, M. E., Schram, K., Elzinga, A., & Zoutendijk, J. (2019). *Alerte burgers, meer veiligheid?: De werking van digitale buurtpreventie in Rotterdam [Alert citizens, more safety?: How digital neighborhood watch works in Rotterdam]*. InHolland. https://surfsharekit.nl/publiek/inholland/87bc7b97-632b-43d0-906e-e68575308f56

Smith, S. A., & Brunner, S. R. (2017). To Reveal or Conceal: Using Communication Privacy Management Theory to Understand Disclosures in the Workplace. *Management Communication Quarterly*, *31*(1), 429–446. https://doi.org/10.1177/0893318917692896

Snyder, J. L., & Cistulli, M. D. (2011). The Relationship Between Workplace E-Mail Privacy and Psychological Contract Violation, and Their Influence on Trust in Top Management and Affective Commitment. *Communication Research Reports*, *28*(2). https://doi.org/10.1080/08824096.2011.565270

Snyder, J. L., & Cistulli, M. D. (2020). Social media efficacy and workplace relationships. *Corporate Communications: An International Journal*, *25*(3), 463–476. https://doi.org/10.1108/CCIJ-01-2020-0006

Solove, D. (2002). Conceptualizing Privacy. *California Law Review*, *90*(4), 1087–1155. https://doi.org/doi:10.15779/Z382H8Q

Solove, D. (2008). *Understanding Privacy*. Harvard University Press.

Stanton, J. M., & Stam, K. R. (2003). Information Technology, Privacy, and Power within Organizations: A view from Boundary Theory and Social Exchange perspectives. *Surveillance & Society*, *1*(2), 152–190. https://doi.org/10.24908/ss.v1i2.3351

Stattin, H., & Kerr, M. (2000). Parental Monitoring: A Reinterpretation. *Child Development*, *71*(4), 1072–1085. https://doi.org/10.1111/1467-8624.00210

Steeves, V. (2009). Reclaiming the social value of privacy. In I. Kerr, V. Steeves, & C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. Oxford University Press.

Steeves, V. (2014, January 22). *Young Canadians in a Wired World, Phase III: Talking to Youth and Parents about Life Online*. MediaSmarts. https://mediasmarts.ca/ycww/talking-youth-parents-about-life-online

Steeves, V. (2015). Privacy, sociality and the failure of regulation: Lessons learned from young Canadians' online experiences. In B. Roessler & D. Mokrosinska (Eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (pp. 244–260). Cambridge University Press.

Steeves, V., McAleese, S., & Brisson-Boivin, K. (2020). *Young Canadians in a Wireless World, Phase IV: Talking to Youth and Parents about Online Resiliency*. MediaSmarts. https://mediasmarts.ca/research-policy/young-canadians-wireless-world/young-canadians-wireless-world-phase-iv/young-canadians-wireless-world-phase-iv-talking-youth-parents-about-online-resiliency

Steimel, S. (2021). Communication Privacy Management and Pregnancy Loss in Interpersonal Workplace Communication. *Women's Studies in Communication*, *Epub ahead of print*, 1–22. https://doi.org/10.1080/07491409.2020.1843579

Steinberg, L., & Silverberg, S. B. (1986). The Vicissitudes of Autonomy in Early Adolescence. *Child Development*, *57*(4), 841–851. https://doi.org/10.2307/1130361

Stephens, K. K., Mandhana, D. M., Kim, J. J., Li, X., Glowacki, E. M., & Cruz, I. (2017). Reconceptualizing Communication Overload and Building a Theoretical Foundation. *Communication Theory*, *27*(3), 269–289. https://doi.org/10.1111/comt.12116

Stoilova, M., Nandagiri, R., & Livingstone, S. (2019). Children's understanding of personal data and privacy online – a systematic evidence mapping. *Information, Communication & Society*, *24*(4), 557–575. https://doi.org/10.1080/1369118X.2019.1657164

Storch, S. L., & Ortiz Juarez-Paz, A. V. (2019). The role of mobile devices in 21st-century family communication. *Mobile Media & Communication*, *7*(2), 248–264. https://doi.org/10.1177/2050157918811369

Subramaniam, M., Kumar, P., Morehouse, S., Liao, Y., & Vitak, J. (2019). Leveraging funds of knowledge to manage privacy practices in families. *Proceedings of the Association for Information Science and Technology*, *56*(1), 245–254. https://doi.org/10.1002/pra2.67

Sultan, A. J. (2014). Addiction to mobile text messaging applications is nothing to "lol" about. *The Social Science Journal*, *51*(1), 57–69. https://doi.org/10.1016/j.soscij.2013.09.003

Sutikno, T., Handayani, L., Stiawan, D., Riyadi, M. A., & Subroto, I. M. I. (2016). WhatsApp, Viber and Telegram which is Best for Instant Messaging? *International Journal of Electrical and Computer Engineering (IJECE)*, *6*(3), 909–914. https://doi.org/10.11591/ijece.v6i3.pp909-914

Tarran, B. (2018). What can we learn from the Facebook—Cambridge Analytica scandal? *Significance*, *15*(3), 4–5. https://doi.org/10.1111/j.1740-9713.2018.01139.x

Teddlie, C., & Yu, F. (2007). Mixed Methods Sampling: A Typology With Examples. *Journal of Mixed Methods Research*, *1*(1), 77–100. https://doi.org/10.1177/1558689806292430

Toorman, A., & Den Engelsman, M. (2009). *Policing in the Netherlands*. Ministry of the Interior and Kingdom Relations: Police and Safety Regions Department. https://www.government.nl/binaries/government/documents/leaflets/2009/01/01/policing-in-the-netherlands/policing-in-the-netherlands.pdf

Trinity McQueen. (2018). *Parenting Digital Natives: Concerns and Solutions*. Internet Matters. https://www.internetmatters.org/wp-content/uploads/2018/01/Internet_Matters_-Parenting_Digital_Natives_Report_2018.pdf

Trottier, D. (2012). Interpersonal Surveillance on Social Media. *Canadian Journal of Communication*, *37*(2), 319–332. https://doi.org/10.22230/cjc.2012v37n2a2536

Van der Land, M., van Stokkom, B., & Boutellier, H. (2014). *Burgers in veiligheid: Een inventarisatie van burgerparticipatie op het domein van de sociale veiligheid [Citizens in safety: An inventory of citizen participation in the field of social safety]* [Report commisioned by Wetenschappelijk Onderzoek- en Documentatiecentrum, Ministry of Safety and Justice, the Netherlands]. Vrije Universiteit. https://www.publicspaceinfo.nl/media/bibliotheek/None/LANDSTOKKO%202014%200001.pdf

Van der Leun, J. P., & Van der Woude, M. A. H. (2011). Ethnic profiling in the Netherlands? A reflection on expanding preventive powers, ethnic profling and a changing social and political context. In L. Weber & B. Bowling (Eds.), *Stop and Search Police Power in Global Context* (Vol. 21, pp. 92–103). Routledge

Van der Veer, N., Boekee, S., & Hoekstra, H. (2021). *Nationale Social Media Onderzoek 2021*. Newcom. https://www.newcom.nl/socialmediaonderzoek/

Van Dijck, J., Poell, T., & De Waal, T. (2018). *The Platform Society: Public Values in a Connective World*. Oxford University Press.

Van House, N. A. (2015). Entangled with technology: Engagement with Facebook among the young old. *First Monday*, *20*(11). https://doi.org/10.5210/fm.v20i11.6311

Van Prooijen, A. M., Ranzini, G., & Bartels, J. (2018). Exposing one's identity: Social judgments of colleagues' traits can influence employees' Facebook boundary management. *Computers in Human Behavior*, *78*, 215–222. https://doi.org/10.1016/j.chb.2017.10.002

Van Rens, M., Haelermans, C., Groot, W., & van den Brink, H. M. (2019). Girls' and Boys' Perceptions of the Transition from Primary to Secondary School. *Child Indicators Research*, *12*(4), 1481–1506. https://doi.org/10.1007/s12187-018-9591-y

Varghese, J. (2009). *Police structure: A comparative study of policing models* (Police Reforms in the Light of Draft Kerala Police Act). Government Law College. https://papers-ssrn-com.eur.idm.oclc.org/sol3/papers.cfm?abstract_id=1605290

Vasalou, A., Oostveen, A.-M., & Joinson, A. N. (2012). A case study of non-adoption: The values of location tracking in the family. *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*, 779–788. https://doi.org/10.1145/2145204.2145321

Vitak, J. (2015). *Balancing privacy concerns and impression management strategies on Facebook*. Symposium on Usable Privacy and Security (SOUPS), Ottawa, Canada. https://cups.cs.cmu.edu/soups/2015/papers/ppsVitak.pdf

Vitak, J. (2016). A digital path to happiness? Applying Communication Privacy Management Theory to Mediated Interactions. In L. Reinecke & M. B. Oliver (Eds.), *The Routledge Handbook of Media Use and Well-Being* (pp. 247–287). Routledge.

Vitak, J., Lampe, C., Gray, R., & Ellison, N. B. (2012). 'Why won't you be my Facebook friend?': Strategies for managing context collapse in the workplace. *IConference 2012*, 555–558. https://doi-org.eur.idm.oclc.org/10.1145/2132176.2132286

Vitak, J., Liao, Y., Kumar, P., Zimmer, M., & Kritikos, K. (2018). Privacy Attitudes and Data Valuation Among Fitness Tracker Users. In G. Chowdhury, J. McLeod, V. Gillet, & P. Willett (Eds.), *Transforming Digital Worlds: IConference 2018* (Vol. 10766, pp. 229–239). Springer International Publishing. https://doi.org/10.1007/978-3-319-78105-1_27

Walden, J. A. (2016). Integrating Social Media Into the Workplace: A Study of Shifting Technology Use Repertoires. *Journal of Broadcasting & Electronic Media*, *60*(2), 347–363. https://doi.org/10.1080/08838151.2016.1164163

Walker, C. R., & Walker, S.-G. (1990). The Citizen and the Police: A Partnership in Crime Prevention. *Canadian Journal of Criminology*, *32*(1), 125–135. https://doi.org/10.3138/cjcrim.32.1.125

Warren, S., & Brandeis, L. (1890). Right to Privacy. *Harvard Law Review*, *4*(5). http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm

Waterloo, S. F., Baumgartner, S. E., Peter, J., & Valkenburg, P. M. (2017). Norms of online expressions of emotion: Comparing Facebook, Twitter, Instagram, and WhatsApp. *New Media & Society*, *20*(5), 1–19. https://doi.org/10.1177/1461444817707349

Watkins Allen, M., Coopman, S. J., Hart, J. L., & Walker, K. L. (2007). Workplace Surveillance and Managing Privacy Boundaries. *Management Communication Quarterly*, *21*(2), 172–200. https://doi.org/10.1177/0893318907306033

Watson, M. (2016). Placing power in practice theory. In A. Hui, T. Schatzki, & E. Shove (Eds.), *The Nexus of Practices* (pp. 169–182). Routledge.

Wei, L. H. (2020, October 29). Is WhatsApp Considered Social Media? *Followchain blog*. https://www.followchain.org/is-whatsapp-social-media/

Westin, A. F. (1967). *Privacy And Freedom*. Atheneum Press.

Wijkagent [Community police officer]. (n.d.). *Politie*. Retrieved 12 January 2018, from https://www.politie.nl/themas/wijkagent.html

Willis, B. (2019, March 3). *How enterprise social media like Slack can improve employee well-being*. The Next Web. https://thenextweb.com/contributors/2019/03/03/enterprise-social-mediaslack-improve-well-being-workplace/

Woermann, N. (2017). Back to the roots! Methodological situationalism and the postmodern lesson for studying tribes, practices, and assemblages. *Marketing Theory*, *17*(2), 149–163. https://doi.org/10.1177/1470593116679869

Wolf, R. D., & Abeele, M. M. P. V. (2020). Editorial: Children's Voices on Privacy Management and Data Responsibilization. *Media and Communication*, *8*(4), 158–162. https://doi.org/10.17645/mac.v8i4.3722

Xu, H., Gupta, S., Rosson, M., & Carroll, J. (2012). Measuring mobile users' concerns for information privacy. *Proceedings of the International Conference on Information Systems 2012 on Digital Innovation in the Service Economy*, 1–16. http://aisel.aisnet.org/icis2012/proceedings/ISSecurity/10

Yesil, B. (2006). Watching Ourselves. *Cultural Studies*, *20*(4–5), 400–416. https://doi.org/10.1080/09502380600708770

YoungWorks. (2014). *Online onderzoek Ouder & Kind [Online research Parent & Child]* [Rapport in opdracht van Mediawijzer.net]. https://www.mediawijzer.net/wp-content/uploads/mw2015/YoungWorks-en-Mediawijzer-rapport-Recht-op-Mediawijsheid.pdf?x68418

Zepan, S., & Črnič, T. O. (2018). From surveillance to co-viewing: Strategies and responses to smartphone regulation within a family context. *Anthropological Notebooks*, *24*(3), Article 3. http://ojs.westeurope.cloudapp.azure.com/Notebooks/article/view/36

Zimmer, M., Kumar, P., Vitak, J., Liao, Y., & Kritikos, K. C. (2020). 'There's nothing really they can do with this information': Unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication & Society*, *23*(7), 1020–1037. https://doi.org/10.1080/1369118X.2018.1543442

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

Appendices

Appendix 1: Interview respondents WNCP groups

Pseudonym	Identifies as	Role	WNCP initiated by	Police involvement	Neighbourhood	Urbanity level (2016)
Pauline	Female	Moderator	Citizen	None	City C	1
Dave	Male	Moderator	Police	Direct	City E	1
Bas	Male	Police				
Marion	Female	Moderator	Police/citizen	Indirect	Suburb M	2
Marc	Male	Moderator	Citizen	None	Suburb D	2
Arnold	Male	Moderator	Citizen	None	Town G	3
Lenny	Male	Moderator				
Kai	Male	Moderator	Citizen	None	Town S	3
Saskia	Female	Moderator	Citizen	Indirect	Suburb H	3
James**	Male	Citizen				
Henry**	Male	Citizen				
Jessica**	Female	Citizen				
Bram**	Male	Citizen				
Daniel**	Male	Citizen				
Emma**	Female	Citizen				
John	Male	Moderator	Citizen	None	Village Z	4
Sven	Male	Moderator	Police	Direct	Town B	4
Klara	Female	Moderator	Citizen	None	Town L	4
Harold	Male	Moderator	Citizen	Indirect	Village H	4
Theo**	Male	Citizen				
Chrissy**	Female	Citizen				
Vera**	Female	Citizen				
Betty**	Female	Citizen				
Lucia**	Female	Citizen				
Bert	Male	Moderator	Citizen	Direct	Village W	5
Ron	Male	Moderator	Police/citizen	Indirect	Village N	5
Louise	Female	Moderator	Citizen	None	Village S	5

Pseudonym	Identifies as	Role	WNCP initiated by	Police involvement	Neighbourhood	Urbanity level (2016)
Rob*	Male	Moderator	Police	Direct	N/A	N/A
Diana*	Female	Moderator	Citizen	None	N/A	N/A
Erik*	Male	Moderator	Citizen	None	N/A	N/A
Richard*	Male	Moderator	Citizen	Indirect	N/A	N/A
Nils*	Male	Moderator	Citizen	None	N/A	N/A
Dan*	Male	Citizen	Citizen	None	N/A	N/A
Eva*	Female	Citizen	Police	Direct	N/A	N/A
Mike*	Male	Citizen	Police	Direct	N/A	N/A
Juliana*	Female	Citizen	Citizen	None	N/A	N/A
Jim*	Male	Police	Citizen	Indirect	N/A	N/A
Bart*	Male	Police	Police	Direct	N/A	N/A
Ron*	Male	Police	Citizen	None	N/A	N/A
Rick*	Male	Police	Citizen	Indirect	N/A	N/A

*Interviews conducted by master's student Frank Holleman (used in Chapter 4)

**Interviewed in focus group setting

Appendix 2: Interview respondents workplaces

Pseudonym	Identifies as	Role	Work context
Lara	Female	Employee office	Graphic design agency
Andrea	Female	Employee office	Consultancy
Tom	Male	Employee office	Multinational
Michael	Male	Employee office	Multinational
Erik	Male	Employee office	Software company
Jay	Male	Self-employed professional	Start-up
Marcus	Male	Self-employed professional	Start up
Lauren	Female	Self-employed professional	Start up
Ciara	Female	Self-employed professional	Start-up
Emily*	Female	Employee service industry	Restaurant
Sarah*	Female	Employee service industry	Restaurant
Jennifer*	Female	Employee service industry	Restaurant
Lea	Female	Manager	Hotel
Mark	Male	Manager	Municipality
Kenneth	Male	Manager	Zoo
Victor	Male	Manager	Government

*Emily, Sarah and Jennifer were interviewed together in a focus group set-up

Appendix 3: Focus group respondents IPAs

Focus group	Pseudonym	Identifies as	Age group	Profession
1	Jessica	Female	20-30	Marketing
	Kim	Female	20-30	PhD candidate
	Peggy	Female	30-40	Education support
	Susan	Female	30-40	Communication
	Henry	Male	40-50	IT
	Charlie	Male	50-60	Professor
2	Bjorn	Male	20-30	PhD candidate
	Kathryn	Female	20-30	PhD candidate
	Julia	Female	20-30	PhD candidate
	Lucas	Male	30-40	Researcher
	Andreas	Male	30-40	PhD candidate
	Alex	Male	40-50	IT
	Marcus	Male	40-50	IT
3	Mark	Male	20-30	Education support
	Hannah	Female	30-40	Education support
	Anna	Female	30-40	Logistics
	Leah	Female	30-40	Organization support
	Jay	Male	40-50	Communication
4	Babette	Female	20-30	Research support
	Marian	Female	20-30	PhD candidate
	Jessie	Female	30-40	Health support
	Karen	Female	30-40	Professor
	Robert	Male	40-50	IT
	Peter	Male	40-50	IT
	Leo	Male	50-60	Professor
5	Claire	Female	30-40	IT
	Linda	Female	30-40	Professor
	Michelle	Female	30-40	PhD candidate
	Dennis	Male	40-50	IT
	Louis	Male	40-50	Library support
6 (conducted in English)	Mona	Female	20-30	PhD Candidate
	Evy	Female	20-30	PhD Candidate
	Jack	Male	30-40	PhD Candidate
	Monica	Female	30-40	Communication
	Leon	Male	30-40	PhD Candidate

Appendix 4: Interview respondents family surveillance

Interview	Pseudonym	Role	Age
Family 1: Mother, father, two sons (11, 13). *Interview setting: Open kitchen / living room, full family present (mother cleaning the house), first interview with father, second with both sons*			
1	Paul	Father	42
2	Parker	Son	13
	Tim	Son	11
Family 2: Single mother, one daughter (12) – daughter spends two weekends a month with her father. *Interview setting: Open kitchen / living room area, mother and daughter interviewed separately while the other person was in the other room*			
3	Nadia	Mother	42
4	Ellie	Daughter	12
Family 3: Mother, father, two daughters (9 , 13), one son (11). *Interview setting: Open kitchen / living room area, daughter interviewed with mother sitting at the same table, parents interviewed together without daughter present, youngest daughter occasionally present.*			
5	Fiona	Mother	44
	George	Father	42
6	Jill	Daughter	13
Family 4: Single father, three sons (9, 14, 16) who spend half of the week wtih their mother. *Interview setting: Open kitchen / living room area, son interviewed with father partly present, father interviewed with son fully present. Other sons came home during interview but did not participate.*			
7	Joel	Father	48
8	Scott	Son	14
Family 5: Mother, father, son (13), daughter (11). *Interview setting: Online (Zoom), interviewed together, son was distracted at times and left the conversation for short breaks.*			
9	Greta	Mother	43
	Jack	Son	13

Interview	Pseudonym	Role	Age
Family 6: Full-time single mother, son (14), daughter (12). *Interview setting: Online (Google Meet), interviewed together, both were fully engaged throughout the interview.*			
10	Abby	Mother	39
	Naomi	Daughter	12
Family 7: Mother, father, daughter (15), son (12). *Interview setting: Online (Teams), interviewed together, daughter came in a bit after the start, the father left two times to take a phone call, all three were engaged.*			
11	Oscar	Father	49
	Grace	Mother	43
	Lucy	Daughter	15
Family 6: Mother, mother, daughter (13), son (9). *Interview setting: Online (Google Meet), interviewed together, both were fully engaged. Son (9) was in the same room but only interrupted twice.*			
12	Camila	Mother	45
	Jasmin	Daughter	13
Family 9: Single mother, foster son (13), foster son (12), foster daughter (11) who spend two days a week with their father. *Interview setting: Open kitchen / living room area, interviewed together, oldest son also present but busy with craft work.*			
13	Lydia	Mother	45
	Eli	Son	12
	Faith	Daughter	11

Appendix 5: Interview and focus group guides WNCP

Moderator interviews[11]

Review and sign consent forms or discuss and ask oral consent (in case of digital interview)

WNCP Group details

- Group active since?
- Number of members?
- Other members than neighbours?

Neighbourhood

- Specific risks / threats in the neighbourhood?

Start WNCP group

- Cause / Origin
- Steps to set up group *(Promotion practices (flyer)*
- Reactions from environment
  (Positive / negative / external objections to group)

Management

- Organization of group(s)
- Which area (e.g., how many streets)
- Single or multiple groups? Set-up?
- Connected to WABP?
- Cooperation between the police / municipality / other groups or districts?
- Which guidelines/rules are used in your group and how are these communicated?
- [after discussion of rules, check ones that are not mentioned] How (if any) did you incorporate the following common rules in your group:
  - *Only for suspicious situations and criminal offenses*
  - *Messages in group need to be 112 worthy*
  - *No jokes and no "pavement tile" notifications (non-emergency content)*
  - *SAAR method?*
  - *Actual place of residence: check or screening if someone is a neighbour?*

[11] This interview guide is translated from Dutch to English for this dissertation, it formed the basis for all interviews. I sometimes added some questions when particular circumstances required this (for instance, for some WNCP groups I knew beforehand that they were interconnected with other groups, so I asked more detailed questions about this at the start)

- *Rules about sharing content of group with others?*
- *How do you deal with sharing pictures in your group chat(s)?*
- *Sensitive information on photos (suspicious persons / license plates)*
- *The other way around scenario (how would you respond if someone would post a picture of you in their WNCP group?)*

Use of group

- What qualifies as important information to share in WhatsApp neighbourhood watch group
- Examples of successes
- Examples of less successful actions
- How would you describe the conversations in your WNCP group
- Tone (e.g., friendly, positive, business-like, negative, extensive)
- What could be objections/risks WhatsApp neighbourhood watch group?
- Can you describe your tasks/practices as a moderator?
- Intervene / advise
- What are the consequences of incorrect actions?
- Do you communicate with WNCP members via other channels? (e.g., Twitter/Facebook/Nextdoor)

Personal information participants

- How do you deal with personal data of participants?
- *Storage and use of participant forms*
- Phone numbers visible in WhatsApp group:
- *Implications? Safeguards?*
- *Use for WhatsApp neighbourhood watch group?*
- *Use for other purposes?*

Personal use of WhatsApp

- How do you react to notifications?
- What if you're not in the neighbourhood?
- When on vacation? At work? How do you deal with WNCP notifications?
- Special settings for group?
- Work communication on WhatsApp?
- Use of WhatsApp settings:
- *Blue Checks / Last Online / Location Settings*
- *Mute/silence?*

- What kind of information do you share in different WhatsApp groups?
- *Information about your location*
- *Information about your relationship status*
- *Information about your position*
- Objections to sharing personal information on WhatsApp?

Extra (if time)

- It was recently announced that WhatsApp wants to share data with Facebook to improve advertisements on Facebook and to be able to make you offers via WhatsApp.
- Response in relation to WNCP?

Focus group guide

Review and sign consent forms before start of conversations

Introduction round

- Explanation of group interview
- *No one on one conversation*
- *General and specific questions aimed at the whole group*
- *More group discussion than interview, asking each other questions, responding to each other.*
- *Introducing new topics or asking for clarification will only benefit the conversation.*
- *The intention that what is discussed within the group interview is not shared with other persons.*
- *Processing of results is completely anonymous.*
- *Common findings are shared with admins, who don't know who joined the conversation*
- Researcher introduction
- Participant introduction:
- *Name (or pseudonym) + indication when joined group*

Motivation for participation WNCP

- Reason to participate in WNCP
- *Risks / threats / reactions from environment*
  (Positive / negative / objections to group?)
- Part of other WNCP groups?

Discussion: WhatsApp neighbourhood watch in general

(prompts: news clippings - hand outs with examples)

- Initial response to:
- *Positive function of group (example Tilburg)*
- *Objections/risks WhatsApp neighbourhood watch group*
- *Aalburg (discrimination)*
- *Eemnes (taking the law into your own hands)*
- What would happen if something like this happened in WNCP group?

Group functioning

- What do you consider to be important information that needs to be communicated via WhatsApp neighbourhood watch group?
- Examples of messages in group?
- Examples of actions? Successes/less sucessful actions?
- How do you respond if pictures are shared in the group?
- Benefits?
- Objections (conversely scenario: photographed yourself in another neighbourhood?)
- Use of rules in WNCP group:
- *How do you experience the rules?*
- *Who intervenes / advises when?*
- *What (if anything) can be changed about this?*
- *Consequences of incorrect actions?*

Personal use

- How do you react to notifications?
- What if you’re not in the neighbourhood?
- When on vacation? At work? How do you deal with WNCP notifications?
- Special settings for group?
- WhatsApp settings: Blue Checks / Last Online / Location Settings / Mute/silence?
- What kind of information do you share in different WhatsApp groups:
- *Information about your location*
- *Information about your relationship status*
- *Information about your position*
- Objections to sharing personal information on WhatsApp?
- How do you feel about visibility phone numbers in WhatsApp?

WhatsApp use in general

- What type of WhatsApp contacts?
- *Neighbours*
- *Colleagues (groups)*
- *Family*
- Different practices across groups?
- Personal WhatsApp settings
- *Blue checks / Last online / Mute / Silence*
- What do you share or not share with whom on WhatsApp?
- *Absence (vacation)*
- *Relationship status*
- *Photos (family)*
- *Address details*

Wrapping up

- Short summary and round with possibility to add more.

Appendix 6: Interview guide workplace communication

Use of different messaging apps /digital work communication platforms

- What does your work look like?
- Use of messaging app part of your typical day
- How do you make distinctions between personal and professional?
- Where do these overlap?

Use of group chats

- Main benefits of group chat apps
- Drawbacks of using group chat apps
- Unwritten rules group chat apps (what is acceptable, what not):
- *Unexpectedly added to group chats*
- *Leaving groups*
- *Adding people to groups*
- *Ignore groups*
- *Appropriate / inappropriate content*

Personal information

- Concerns sharing personal information on group chat apps
- *Avoiding apps for this reason*
- *Differences between apps*
- Information that you deliberately do not share with colleagues
- *Phone number, home address, bank account no., date of birth*
- *Personal life: when you are home and away, leisure activities, relation status*
- Differences in sharing of personal info between personal and professional use
- Professional information you want to protect
- Sharing pictures (what to share and not to share)
- WhatsApp: Phone numbers visible of all group members
- *Use outside group*
- Facebook: Linked to personal Facebook account
- *Approaching colleagues outside of work group chat*
- A while ago, WhatsApp announced to share user data with Facebook to improve Facebook advertising and to offer targeted advertisements via WhatsApp.
- Privacy concerns?

Personal reactions / use / settings

- Specific privacy settings
- Reaction to notifications of work messages
- Reaction speed
- Outside office hours
- Evening
- Weekend
- Holiday

Specific settings

- Mute groups
- Different sounds for different notifications
- Location setting phone
- WhatsApp - Blue checks / Last seen

Appendix 7: IPA survey questions / focus group guide

IPA survey questions

Demographics

You identify as:

- Male
- Female
- Nonbinary / Gender non-conforming / Third gender
- Prefer to self-describe:
- Prefer not to answer

How old are you today, in years?

What is the highest level of education you have completed?

- Less than high school
- High school graduate, diploma or the equivalent (GED)
- Some college credit, no degree
- Trade/technical/vocational training
- Associate degree
- Bachelor's degree
- Master's degree
- Post-graduate degree (e.g., PhD, MD, JD)
- Prefer not to answer

Including yourself, how many people live in your household?

What is your annual household income?

- Less than € 25.000
- € 25.000 - € 40.000
- € 40.001 - € 50.000
- € 50.001 - € 65.000
- € 65.001 - € 85.000
- € 85.001 - € 130.000
- More than € 130.000
- Prefer not to answer

Internet familiarity

How familiar are you with the following Internet-related terms?

Respond based on your ability to explain or describe this term to another person.

(Response options: No Understanding / A Little Understanding / Some Understanding / Good Understanding / Full Understanding)

- Advanced search
- Tagging
- PDF
- Spyware
- Wiki
- JPG
- Weblog
- Cache
- Malware
- Phishing

Digital literacy (related to smartphone use)

How confident are you about doing the following tasks on your smartphone?

(5 response options: Not at All Confident / A Little Confident / Somewhat Confident / Moderately Confident / Very confident)

- Sending photos taken with my phone to other people.
- Adjusting which apps have permission to access my microphone.
- Changing my location privacy settings.
- Updating my phone to the newest operating system.
- Sharing my location with someone else through my phone.
- Downloading music to my phone.
- Creating a personal hotspot with my phone.
- Changing the access code / password on my phone.
- Deleting an app from my phone.
- Connecting another device to my phone using Bluetooth.
- Sending photos taken with my phone to other people.
- Adjusting which apps have permission to access my microphone.
- Changing my location privacy settings.
- Updating my phone to the newest operating system.
- Sharing my location with someone else through my phone.

- Downloading music to my phone.
- Creating a personal hotspot with my phone.
- Changing the access code / password on my phone.
- Deleting an app from my phone.
- Connecting another device to my phone using Bluetooth.

General privacy concerns

Indicate your level of concern about the following scenarios that might happen when you use communication technologies (e.g., social media, email, apps).

(5 response options: Not at All Concerned / Slightly Concerned / Somewhat Concerned / Moderately Concerned / Extremely Concerned)

- Your account being hacked.
- Your picture being used in a social media ad.
- Receiving inappropriate messages (e.g., naked photos) from another user.
- Being tagged in a photo you don't want linked to your profile.
- Being tagged in an update that identifies your current physical location.
- Personal account information being compromised / leaked (e.g., your email and password get posted online).
- Someone posting a mean, unflattering, or factually incorrect update about you.
- Your employer viewing content (text or photos) that might negatively impact your job.
- Your personal information being sold to other companies for marketing purposes.
- Private messages becoming publicly visible.
- Unwanted contact from another user.
- Your personal information (phone number, address, etc.) becoming publicly visible.

Mobile privacy concern

How much do you agree or disagree with the following statements about your use of mobile phone apps?

(5 response options: Strongly Disagree / Somewhat Disagree / Neutral / Somewhat Agree / Strongly Agree)

- I believe that the location of my mobile device is monitored at least part of the time.

- I am concerned that mobile apps are collecting too much information about me.
- I am concerned that mobile apps may monitor my activities on my mobile device.
- I feel that as a result of my using mobile apps, others know about me more than I am comfortable with.
- I believe that as a result of my using mobile apps, information about me that I consider private is now more readily available to others than I would want.
- I feel that as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy.
- I am concerned that mobile apps may use my personal information for other purposes without notifying me or getting my authorization.
- When I give personal information to use mobile apps, I am concerned that apps may use my information for other purposes.
- I am concerned that mobile apps may share my personal information with other entities without getting my authorization.

Mobile privacy confidence

To what extent do you agree or disagree with the following statements? (5 response options: Strongly Disagree / Somewhat Disagree / Neutral / Somewhat Agree / Strongly Agree)

- I am confident that my phone’s apps only access data from my phone necessary to perform a specific service.
- I know what data each app on my phone collects about me.
- I am confident in my ability to control how individual apps access personal data on my phone.
- I am not concerned about the data my phone collects because none of it is sensitive

Household IPA familiarity

Have you heard of the following intelligent personal assistant devices (also known as smart speakers)? (3 response options: Yes / No / Not Sure)

- Google Home / Home Mini
- Amazon Echo / Echo Dot
- Apple HomePod

Household IPA privacy concerns

Please read the following statements. Indicate your current or likely response about concerns with IPAs (even if you've never owned or used an IPA device).
(5 response options: Not at All Concerned / Slightly Concerned / Somewhat Concerned / Moderately Concerned / Extremely Concerned)

- I am concerned that the device is always listening.
- I am concerned that the device is always recording any sounds in the room.
- I am concerned that other people might activate/access the device and trigger unauthorized purchases.
- I am concerned that other people might activate/access the device and disrupt my internet accounts or personal information.
- I am concerned that my questions directed at the device are stored and might be accessed by law enforcement.
- I am concerned that my questions directed at the device are stored and used by the service provider (e.g., Google, Amazon) to predict my interests and future needs.
- I am concerned that my questions directed at the device are stored and sold to third parties (e.g., advertisers).

Smartphone reliance

- How often do you access/use your smartphone throughout a normal day, for any reason?
  Answer via slider scale from Never (0) to Constant (100)
- If you realised after leaving the house for the day that you'd forgotten your phone, how would you feel?
  Answer via slider scale from Not at All Anxious (0) to Very Anxious (100)

IPA focus group guide

Consent forms signed and handed in before start of conversation.
Emphasis during conversation on interaction between participants, questions used as prompts when needed.

Opening

- Welcome, introduction moderators, procedures, and topics

Introductions

- First name and indication of whether you closely follow technological developments or not at all. E.g., gadgets like Google Home, fitness tracking devices such as Fitbit, or do you want to use the newest mobile phone?

Influence of technology (optional!)

- Share thoughts about influence of technology on life. Think about last 5 years, how did technology change daily life?
- At work or at home? Convenient, harmful or annoying? Why?

IPAs on phone

- Intelligent personal assistants: First, voice-activated assistant on mobile phone. Does anyone use Siri, Google Assistant, Microsoft Cortana or similar service?
- Example of uses? Why IPA and no other means?
- Never used? Why not?
- Benefits?
- Drawbacks?

Smart speakers

- Smart speakers: any associations by Amazon Echo, Google Home or Apple HomePod?
- Does anyone own such a device? For which tasks / activities?
- Who knows what these devices can do?
- Google Home expected later this year in NL,
- Activity: watch Google Home commercial as introduction prompt

Interactive activity – participants try-out device

- Try out – start with OK Google or Hey Google, some suggestions on paper:
- *Turn on the lamp*
- *Sing me a song*
- *Play a Hip-hop song on Spotify*
- *What is the weather forecast for Rotterdam this evening?*
- *Find me the nearest Italian restaurant*
- *How can I get to Rotterdam central station by public transport?*
- *Ask me a riddle*
- *Schedule my doctor's appointment for Thursday at 11*
- How do you feel when you interact with Google Home?
- What strikes your attention?
- (Future) uses of these devices?

- Convenient or helpful? Why?
- See yourself buying one in the future? Why (not)?
- For what type of tasks / activities? Work, in the house, in traffic?

Benefits and drawbacks household IPAs

- Benefits devices like Google Home?
- Possibilities to connect with online accounts and services?
- Agenda?
- Other devices? Lights, TV, fridge?
- Drawbacks?
- When do devices listen?
- Only when you use the ‘trigger word’ or always?
- Are there things you don’t want to share with a household IPA?
- Thoughts about data collection?
- Information sharing with mother company
- Different when it’s Google, Amazon or Apple?
- Concerns peers?
- Connected services (Netflix, Spotify)
- Ideas about registration of when you watch/listen, turn on the light?
- Connect to agenda?
- Predictive functions of IPAs? *E.g., phone can see meeting in agenda at 9 and Google Home will tell you that there is a traffic jam and advises you to take a different route to work.*
- Additional benefits and/or drawbacks?

IoT

- Connected to other technologies - Internet of Things
- Examples of smart and connected devices in use?
- Smart TV, smart fridge, washing machine?
- Views on interconnected devices?
- Ideas about predictive functions of interconnected appliances and devices? *E.g., smart fridge knows that you’ve run out of milk and automatically adds it to your Google Home shopping list.*

Inventory of other ideas or topics that came up during conversation

- Wrapping up

Appendix 8: Interview guides family surveillance

Interview guide parents

Introducing myself: PhD research about daily use of communication technologies such as WhatsApp and voice activated smart speakers in different contexts. After looking at neighbourhoods, work environments, and households, my latest research focuses specifically on families. I don't have a background in pedagogy but I'm a media researcher and have toddlers myself, so I have no ideas or judgments about how you should do it as a parent, I'm just really curious about how different technologies are handled in different families.

Review and sign consent forms or discuss and ask oral consent (in case of digital interview)

Introduction

- Can you tell me a bit about yourself? What kind of work do you do? How old are you? What do you use your mobile phone for most?

Family life in times of Covid-19

- Of course, we are now in a pandemic / lock-down situation, can you tell me a bit about what a week in your family looks like?
- Are you dealing with working from home? How do you or did you organise this?
- How did you organise home education when schools were closed?
- In what way (if any) has your use of social media/messaging apps changed compared to the situation before corona?
- More or less use of devices?
- Can you tell me about the distribution of devices among family members?
- How (if so) has digital communication within the family changed?

Social media/digital oversight

- Do you use social media?
- Which one do you use the most often?
- What do you do most on [most often used platform]?
- How often?
- Who can see what you share?
- Which things do you refrain from sharing on social media?
- Do your children use social media?

- Can you tell me about their social media practices?
- Which? Own account? Through what devices?
- Insight into the use of social media by children?
- How do you get this insight?
- What do you keep an eye on?
- What they post on social media?
- Their interactions on social media? (public and DMs)
- How you establish agreements about the use of social media?
- What?

Online safety?

- Things you don't want them to post?
- To what extent do you have insight into the settings of their accounts?
- Do you know how they act if they are approached by strangers?
- How do your kids keep in touch with friends?
- Via WhatsApp/Snapchat/social media?
- Rules or discussions about online conversations?
- Direct insight in their use of messaging apps?
- How (if so) do you keep track of what your kids are doing online?
- Internet use? Search history?
- YouTube videos?
- How do communicate about where your children are?
- Or how do you keep an eye on where your children are?
- How?
- When?
- To what extent are the children aware of what you know about their online behaviour and location?
- In relation to school – how do you make use of Magister (or a similar service?)
- What do you check?
- What not?

Family communication

- Which family members mobile phone?
- From what age?
- How do you handle mobile phones in your family?
- Agreements about the use of mobile phones? (restrictions?)
- How arranged in terms of mobile subscriptions / WiFi use

- How do you keep contact when family members are not at home?
- Family WhatsApp chat?
- How often used?
- Who messages most often in the family chat?
- Can you please open the family chat or tell me in general about your practices:
- Which topics have been discussed in the family chat in the past two weeks? *No details needed, curious about subjects and moments – dinner/photos/etc.*
- Agreements about using a group app?
- Topics (not) allowed in app?
- Cases of uncertainty about something shared in the app group?
- Benefits and drawbacks?

Smart technologies

- Do you use a smart assistant on your phone? (e.g., Siri, Google Assistant, Bixby)
- If yes, can you tell me how you use it?
- Do you have smart devices at home? Yes > Such as?
- Smart door lock, smart TV, robot vacuum cleaner, smart lamps, smart doorbell?
- Devices you can talk to? Such as Smart speakers (Google Home, Amazon Echo)

Yes >>

- How often do you use these devices?
- Advantages compared to 'dumb' devices?
- Where do you use them for? *Lamps, curtains / Spotify /Netflix / PostNL packages / Bol.com orders / Home delivery?*
- Which one of you uses these most often?
- Who installed them? Who connected them? Are they linked to a particular account?
- Did you establish any agreements about the use of devices?
- Things kids shouldn't do?
- Things you consciously do not use smart speakers for?
- Mute?
- What kind of data does smart speaker collect?
- Insight into what smart speaker knows?

- Specific settings?

No >>

- Would you consider purchasing smart devices in the future?
- Advantages of turning on lights, music, TV series via voice?
- Cons? Things you wouldn't share with a smart speaker?

Interview guide children (translated from Dutch to English for this dissertation)

Introducing myself: Research about how people stay connected in neighbourhoods, at work, and at home, and about smart devices you can turn on by saying something to them. And this research is about staying connected and smart devices in families. I have very small children of my own, ages 1 and almost 3, and they only use my phone for YouTube Kids and the Miffy app so I think I can learn a lot about social media and your mobile phone use from you!

Review and sign consent forms together with parent or discuss and ask oral consent (in case of digital interview)

Introduction

- Can you tell me something about yourself? How old are you? What is your favourite activity?

Family life in times of Covid-19

- Of course, we are now in a corona lock-down, can you tell me what do you notice about that at the moment?
- Did you take or are you taking online classes from home? What is/was the school day like at home?
- How often can you now go to school and how often do you have to take classes online?
- What do you like most about going to school? What have you missed?
- Did your parents work from home or do they work from home?
- How did it go? Who worked where?
- How did you keep in touch with friends from school?
- Can you make an estimation if you used your devices more or less often in the past year than before Covid-19?

Social media use

- Which apps do you use most often?
- For what do you use it?

- How often?
- Which (if any) social media apps? (Facebook, Twitter, Tiktok, Instagram)
- Which social media the most?
- Own account?
- What do you use social media for?
- Who can see your posts?
- Are there things you deliberately don't share on social media? What?
- Do friends share things you wouldn't share?
- Can you tell me about any agreements with parents about what is and is not allowed on social media?
- Can you tell me if and how social media is discussed at school?
- Do your parents know what you do on social media? What do you notice about that?
- How do you keep in touch with friends or other contacts?
- *Via WhatsApp/Snapchat/Discord/Messenger?*
- Are there things you deliberately don't share via messaging app?
- Do friends ever share something you wouldn't share?
- If you get messages from someone you don't know, what do you do?
- Do parents know what messages you send and to whom?
- If yes > In what way do they check this? How do you normally respond to that?
- If no > Do you have any friends whose parents check up on their messaging? How do they do this and how does your friend respond?
- Do parents know what you look up on the internet? Watch on YouTube?
- If yes, how? Your response?
- If no, what about friends?
- *Do parents know which games you play? If yes, how? Your response? If no, what about friends?*
- In general, how often do you describe the use of your mobile phone?
- Are there any rules you need to follow? (messaging, gaming, screen-time, etc.)
- Do you experience differences in how your parents deal with your mobile phone compared to other parents? What are the differences?
- Have you ever discussed privacy with your parents or at school? What

does privacy mean to you?

- If you're not at home, how do your parents know where you are?
- Communication? Location tracking?
- Yes? How do you respond to this tracking?
- Can you tell me about how you use Magister for school?
- And can you tell me how your parents use it?

Family communication

- How do you keep contact with your parents when you are away?
- Family WhatsApp chat? How often used?
- Can you please open the family chat or tell me in general about your practices: Which topics have been discussed in the family chat in the past two weeks? *No details needed, curious about subjects and moments – dinner/photos/etc.*
- Agreements about using a group app?
- Topics (not) allowed in app?
- Uncertainty about something shared in the app group?
- What is the best thing about using a group app?
- What is maybe less nice?

Smart technologies

- Are there any smart devices you would like to have?
- Do you have smart devices at home? *Smart door lock, smart TV, robot vacuum cleaner, smart lamps, smart doorbell?*
- Devices you can talk to? Such as Smart speakers (Google Home, Amazon Echo)
- Do you ever do that?
- What do you ask your device? *Jokes / Questions for homework / Control lights / Spotify / Netflix*
- What works well and what doesn't?
- Who installed the device?
- Who decides what is and is not allowed?
- Do you know if the devices are linked to a particular account?
- Agreements about the use of devices?
- Things that are not allowed?
- Mute?
- What does the smart speaker know about you?

Appendix 9: Consent forms

Consent form neighbourhood interviews[12]

Project	**Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems: Practices and Contexts in the Netherlands and US** *This project is funded by NWO from PRICE grant 628.001.024.* This research project has been approved by ESHCC Ethics Review Committee.
Contact	**Anouk Mols,** PhD candidate at Erasmus School of History, Culture and Communication, Department of Media and Communication, mols@eshcc.eur.nl
Research purpose	This study is conducted by Anouk Mols, MSc. The research focuses on the use of WhatsApp neighbourhood crime prevention (WNCP) groups. We would like to investigate how WNCP moderators think about sharing (personal) information with their neighbours. The results of this research are used for scientific productions; for example meetings, publications and possible follow-up research.
Procedure	Your commitment to participate in this research means that you agree to be interviewed about your use of a WNCP group. The interview will last approximately 45 minutes, and you will be asked questions about how you manage the WNCP, what information is shared and your view on this information. If you give permission, an audio recording of the interview will be made.
Risks	There are no physical, regulatory, or economic risks associated with participating in this research.
Confidentiality	In this study, your privacy will be safeguarded. Your information is being handled confidentially, and will only be used for research purposes. The interview data will only be accessed by trained researchers. No personally identifiable information will be reported in any research product. Research results can be shared with you at your request (within the abovementioned limitations). The audio recordings will be transcribed. When segments of the transcripts are used in publications and reports, pseudonyms will be used. The recordings, transcriptions and forms will be stored carefully. After ten years, this information will be destroyed.

[12] This consent form was slightly adjusted for the two focus groups.

Participant rights	Participating in this study is voluntary. You can refuse to answer questions or to end the interview at all times.	
Questions or concerns	In case you have any questions, concerns or complaints, or if you want to stop taking part in the study, please contact the primary investigator: **Jason Pridmore** (Associate professor Media & Communication): pridmore@eshcc.eur.nl. For research problems or questions about data collection, please contact: **Marlon Domingus** (data protection officer): fg@eur.nl.	
Statement of consent	Your signature indicates that you are at least 18 years of age; you have read this consent form or have had it read to you; your questions have been answered to your satisfaction and you voluntarily agree that you will participate in this research study. You will receive a copy of this consent form.	
Audio recording	I consent to have my interview audio recorded: □ YES □ NO	
Signature and date	Name	
	Signature	
	Date	

Consent form workplace interviews

Project	**Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems: Practices and Contexts in the Netherlands and US**. *This project is funded by NWO from PRICE grant 628.001.024.* This research project has been approved by ESHCC Ethics Review Committee.
Contact	**Anouk Mols,** PhD candidate at Erasmus School of History, Culture and Communication, Department of Media and Communication, mols@eshcc.eur.nl
Research purpose	This study is conducted by Jason Pridmore, PhD, Daniel Trottier, PhD and Anouk Mols, MSc. The research aim is to examine the use of mobile group chat applications (WhatsApp, Facebook Messenger, Slack, Google Hangouts etc.). We want to study how users of mobile group chat applications think about sharing (personal) information with their colleagues. The results of this study will be used for academic productions, such as conference presentations, publications and reports.

Procedure	Taking part in this study means that you accept to be interviewed about your use of mobile group messaging applications. The interview will take approx. 45 minutes, and we will ask you questions about when you use mobile group messaging apps to contact your colleagues, what types of information you share, and about your view on sharing personal information. The interview will be audio recorded.	
Risks	There are no physical, regulatory, or economic risks associated with participating in this research.	
Confidentiality	In this study, your privacy will be safeguarded. Your information is being handled confidentially, and will only be used for research purposes. The interview data will only be accessed by trained researchers. No personally identifiable information will be reported in any research product. Research results can be shared with you at your request (within the abovementioned limitations). The audio recordings will be transcribed. When segments of the transcripts are used in publications and reports, pseudonyms will be used. The recordings, transcriptions and forms will be stored carefully. After ten years, this information will be destroyed.	
Participant rights	Participating in this study is voluntary. You can refuse to answer questions or to end the interview at all times.	
Questions or concerns	In case you have any questions, concerns or complaints, or if you want to stop taking part in the study, please contact the primary investigator: **Jason Pridmore** (Associate professor Media & Communication): pridmore@eshcc.eur.nl. For research problems or questions about data collection, please contact: **Marlon Domingus** (data protection officer): fg@eur.nl.	
Statement of consent	Your signature indicates that you are at least 18 years of age; you have read this consent form or have had it read to you; your questions have been answered to your satisfaction and you voluntarily agree that you will participate in this research study. You will receive a copy of this consent form.	
Audio recording	I consent to have my interview audio recorded: □YES □ NO	
Signature and date	Name	
	Signature	
	Date	

Consent form IPA online survey

Project	**Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems: Practices and Contexts in the Netherlands and US.** *This project is funded by NWO from PRICE grant 628.001.024.* This research project has been approved by ESHCC Ethics Review Committee.
Study	The (anticipated) use of Intelligent Personal Assistants (IPAs)
Contact	**Anouk Mols,** PhD candidate Erasmus School of History, Culture and Communication, Department of Media and Communication, mols@eshcc.eur.nl
Purpose of the Study	This research is being conducted by dr. Jason Pridmore, dr. Daniel Trottier and Anouk Mols at the Erasmus University Rotterdam, in collaboration with dr. Jessica Vitak (University of Maryland) and dr. Michael Zimmer (University of Wisconsin-Milwaukee). We are inviting you to participate in this research about how people use interactive, voice-activated technologies like Siri, Alexa, and Google Home.
Procedures	As part of this study, you will be asked to complete a short (10 minute) survey through the survey site Qualtrics. The survey will ask you general questions about your background, use of different smartphone-enabled devices, and your attitudes toward data sharing online. At the end of the survey, you will be invited to enter your email if you are interested in participating in a follow-up interview to further discuss your attitudes toward new interactive technologies being released to the public. In order to participate, you must (1) be at least 18 years old, (2) a Dutch resident, and (3) currently own a smartphone.
Potential Risks	There are no obvious physical, legal or economic risks associated with participating in this study; however, you are free to discontinue participation in the study at any time.
Potential Benefits	Participation in this study does not guarantee any beneficial results. However, you may gain a better understanding of your use of your smartphone and what is done with your personal information online.
Compensation	All survey participants will be invited to provide their email to be entered into a random drawing for one of three €50 Bol.com gift cards. Your email address will not be linked to your responses.

Confidentiality	Copies of the survey data will be retained by the researchers for three years after publication of any results. Data will be stored by the researchers in password-protected files and password-protected email accounts that are only accessible by the researchers. To ensure data confidentiality, each participant will be assigned an ID (e.g., P303) and any identifying information (e.g., name, email) will be removed from the dataset prior to analysis. All collected written documents or written notes will be stored in a locked cabinet in a locked office at department of Media & Communication at Erasmus University. Only the researchers will have access to this cabinet. Your privacy will be protected to the maximum extent allowable by law. No personally identifiable information will be reported in any research product. Moreover, only trained research staff will have access to your responses. Within these restrictions, results of this study will be made available to you upon request. Your information may be shared with representatives of the Erasmus University or governmental authorities if you or someone else is in danger or if we are required to do so by law.
Right to Withdraw	Your participation in this research is completely voluntary. You may choose not to take part at all. If you decide to participate in this research, you may stop participating at any time. If you decide not to participate in this study or if you stop participating at any time, there will be no consequences.
Questions	In case you have any questions, concerns or complaints, or if you want to stop taking part in the study, please contact the primary investigator: **Jason Pridmore** (Associate professor Media & Communication): pridmore@eshcc.eur.nl. For research problems or questions about data collection, please contact: **Marlon Domingus** (data protection officer): fg@eur.nl.
Participant rights	If you have questions about your rights as a research participant or wish to report a research-related injury, please contact: privacy@eur.nl
Statement of Consent	By completing and submitting this online survey, you indicate your voluntary agreement to participate in this research and have your answers included in the data set.

Consent form IPA focus groups

Project	**Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems: Practices and Contexts in the Netherlands and US** *This project is funded by NWO from PRICE grant 628.001.024.* This research project has been approved by ESHCC Ethics Review Committee.
Study	The (anticipated) use of Intelligent Personal Assistants (IPAs)
Contact	**Anouk Mols,** PhD candidate at Erasmus School of History, Culture and Communication, Department of Media and Communication, mols@eshcc.eur.nl
Purpose of the Study	This research is being conducted by dr. Jason Pridmore, dr. Daniel Trottier and Anouk Mols at the Erasmus University Rotterdam, in collaboration with dr. Jessica Vitak (University of Maryland) and dr. Michael Zimmer (University of Wisconsin-Milwaukee). We are inviting you to participate in a focus group about interactive, voice-activated technologies like Siri, Alexa, and Google Home. We want to know about your attitudes toward and knowledge of these devices and the data they collect. The results of this study will be used by the project for conference presentations, reports, and publications.
Procedures	The focus group will take approx. 60-minutes. The moderator will ask you and other participants to discuss the (anticipated) use of interactive personal assistants. During the focus group, you can try out a Google Home device. We will audio record the focus group discussion to facilitate analysis by the research team.
Potential Risks	There are no physical, legal or economic risks associated with participating in this study. Participation is voluntary and you are free to decide not to answer specific questions.
Potential Benefits	There are no direct benefits to the participants. However, we hope that others may benefit from this research through enhanced privacy policies and/or tools that assist users in better understanding how companies collect and use their data.
Compensation	At the end of the session, you will receive a €10,- Bol.com gift certificate.
Confidentiality participants	It is not allowed to discuss the contents of the focus group with other persons outside of the focus group setting.

Confidentiality researcher	We will make every attempt to protect your personal information and privacy. Your information will be treated confidentially and will only be used for research purposes. Only trained researchers will have access to the interview data and no personally identifiable information will be reported in any research product. Within these restrictions, results of this study will be made available to you upon request. The sound recording of this interview will be transcribed. We will pseudonymise personal details when parts of the transcripts are used in research products. Forms and files with identifiable information will be destroyed within one year after the data collection. All collected written documents or written notes will be stored in a locked cabinet in a locked office at department of Media & Communication at Erasmus University. All digital files will be saved in password protected research environments. This information will be destroyed after 10 years.	
Participants rights	Your participation in this research is completely voluntary. If you decide to participate in this research, you may stop participating at any time. If you have questions about your rights as a research participant or wish to report a research-related injury, please contact: privacy@eur.nl.	
Questions	In case you have any questions, concerns or complaints, or if you want to stop taking part in the study, please contact the primary investigator: **Jason Pridmore** (Associate professor Media & Communication): pridmore@eshcc.eur.nl. For research problems or questions about data collection, please contact: **Marlon Domingus** (data protection officer): fg@eur.nl.	
Statement of consent	Your signature indicates that you are at least 18 years of age; you agree to have your comments audio recorded; you have read this consent form or have had it read to you; your questions have been answered to your satisfaction and you voluntarily agree that you will participate in this study. You will receive a copy of this consent form.	
Audio recording	I consent to have this interview audio recorded: □ YES □ NO	
Signature and date	Name	
	Signature	
	Date	

Consent form family surveillance[13]

Project	**Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems: Practices and Contexts in the Netherlands and US.** *This project is funded by NWO from PRICE grant 628.001.024.* This research project has been approved by ESHCC Ethics Review Committee.
Contact	**Anouk Mols,** PhD candidate at Erasmus School of History, Culture and Communication, Department of Media and Communication mols@eshcc.eur.nl
Research purpose	On the basis of interviews, we investigate how different families use communication services (such as WhatsApp) and smart devices (such as smart speakers) and what role this plays in daily family life.
Procedure	The (family or individual) interview will last approximately 60 minutes and will cover communication within the family, the use of smart devices, and the protection of personal information. During the interview you will also be asked if you want to share what is being shared in the family WhatsApp group (if applicable), sharing this content is not mandatory and will only be reported in general terms. An audio recording of the interview will be made.
Risks	There are no physical, regulatory, or economic risks associated with participating in this research.
Benefits	Participation in this study has no direct benefits, although participation may contribute to awareness about technology use within the family.
Reward	Participation in this survey is rewarded with a gift voucher from a webshop of your choice of € 15 per completed interview. I have received this gift voucher: □ YES
Sharing research results	If you wish, we will keep you informed of research results and publications by e-mail over the next three years.
Participant rights	Participating in this study is voluntary. You can refuse to answer questions or to end the interview at all times.

[13] Children received a simplified version of this consent form.

Confidentiality	In this study, your privacy is fully guaranteed to the extent permitted by law. Your data will be treated confidentially and will only be used for research purposes. The audio recordings of this interview will be transcribed. These transcripts and recordings are not shared with other family members. The audio recordings, transcripts, and consent forms are carefully stored in a secure digital environment and will be destroyed in 10 years. The interview recordings will be used for scientific productions such as presentations and publications and for possible follow-up research by the researchers Anouk Mols and Jason Pridmore. No personally identifiable information is reported and when we quote you we use a pseudonym. Your contact details will be deleted after six months, or after three years if you want to be informed about the research results.	
Questions or concerns	In case you have any questions, concerns or complaints, or if you want to stop taking part in the study, please contact the primary investigator: **Jason Pridmore** (Associate professor Media & Communication): pridmore@eshcc.eur.nl. For research problems or questions about data collection, please contact: **Marlon Domingus** (data protection officer): fg@eur.nl.	
Statement of consent	Your signature indicates that you are at least 18 years of age; you have read this consent form or have had it read to you; your questions have been answered to your satisfaction and you voluntarily agree that you will participate in this research study. You will receive a copy of this consent form.	
Audio recording	I consent to have my interview audio recorded: □YES □ NO	
Signature and date	Name and signature	
	Date	

Appendix 10: Chapter 3 Codebook

Selective code	Axial code	Sample of open codes (verbatim)*
Community co-veillance	Social support	Social activities neighbours
		Helping neighbours
	Sense of community	Social cohesion WNCP
		Face-to-face contact
	Social control	Keeping a distance
		Social control unwanted
Scripted moderation	Daily tensions WNCP content	Irrelevant content
		Reprimanding members
	Non-safety related content allowed	Missing pet alert
		Lost keys message
	Moderator efforts and guidelines	Removing members
		Guidelines in manual
Vigilant citizens	Active neighbours	Photograph suspicious activity
		Confronting suspicious persons
	Privacy in neighbourhood	Privacy passer's by harmed
		Picture sharing privacy risk
	Suspicious towards neighbours	Monitoring neighbours
		Following runner at night
Normalised distrust	Multidimensional WNCP networks	Supra-moderators
		Multiple groups in network
	Collaborative efforts	Separate group with moderators
		Active involvement police
	Discriminatory practices	Suspicion based on appearance
		Wrongful accusation

* From a total of 175 open codes

Appendix 11: Chapter 4 Codebook

Selective code	Axial code	Sample of open codes (verbatim)*
Maintaining awareness and noting suspicions	Being alert	Neighbourhood alertness
		Follow intuition
	Assisting police	Police instructions
		Collaborative action with police
	Monitoring neighbours	Watching neighbours’ children
		Evening walk neighbourhood
Alerting (police) about suspicions	Hesitating to contact police	Afraid false alarm
		Alert neighbours before police
	Intolerant practices	Acting on prejudice
		Suspicion based on appearance
Informing WNCP network	Lack of diversity group	Multiculti less involved
		Elderly no WhatsApp
	Gatekeeping practices	Reject application
		Moderator removing members
	Police involvement	Police not in group
		Police active in group
Reacting and acting	Collaborations with police	Collaborative action with police
		Assist in police practice
	Cautious attitudes	Careful taking action
		Avoid getting carried away
	Unrestrained action	Taking action after WNCP alert
		Photograph suspicious activity

* From a total of 175 open codes

Appendix 12: Chapter 5 Codebook

Selective code	Axial code	Sample of open codes (verbatim)*
Demarcating absence and presence	Activating silent mode for temporary absence	The joy of being unavailable Phone always on Notifications cause distraction
	Being visibly present	Last seen setting useful Last seen causes unrest Last seen switched off
	Response accountability	Blue checks avoidance strategy Blue checks cause pressure Blue checks reprimanded
Segmenting relational contexts	Context segmentation	Do-not-disturb exception family Work messaging night not OK Postpone messages to morning
Sculpting WhatsApp boundaries	Managing communication overload	Messages managing strategies Unread to keep track Archiving to maintain control Different sounds for different contexts
	Prioritising contexts	WNCP special settings Muting particular groups

* From a total of 312 open codes

Appendix 13: Chapter 6 Codebook

Professional role	Axial code	Sample of open codes (verbatim)*
Across roles	Strict boundaries	Work separate phone
		Shield personal information
	Permeable boundaries	Work messaging on private phone
		Work/private merging okay
	Safety risks	WhatsApp safer than Facebook
		Use two-factor-authentication
Managers	Private information considerations	WhatsApp more informal than email
		WhatsApp no religious/political content
	Professional role tension	Work WhatsApp manager excluded
		Manager vulnerability mixing contexts
Office employees	Professional nature of communication	Work WhatsApp mainly work related
		Work WhatsApp for inspiration/ news
	Company culture	Weekend no workplace communication
		Work WhatsApp not obliged
Service -industry employees	Turbulence workplace communication	Work messaging inappropriate content
		Private messaging incident
	Social media face risk	Social media control over tagging
		WhatsApp risk picture forwarding
Self-employed professional	Flexible distributed communication	Multiple communication apps
		Flexibility international collaborations
	Social media business	WhatsApp customer communication
		Social media to promote work

* From a total of 291 open codes

Appendix 14: Chapter 7 Codebook

Selective code	Axial code	Sample of open codes (verbatim)*
Surveillance concerns	Household IPA listening	Household IPA always listening Household IPA listening problematic
	Interconnected households	Smart lights Household IPA like science fiction
	Intimate spaces	No household IPA in bedroom Household IPA invades personal space
	Anti-surveillance strategies	Household IPA switched off Household IPA temporarily muted
	Household IPA camera	Household IPA camera no camera Camera creepy
Security concerns	Fear of break-ins	Interesting for burglars Fear of break-ins
	Distrust IPA security	Household IPA technique underdeveloped Link to other devices unsafe
	Security data risks	Fear of hackers Unauthorized purchases household IPAs
	Trust in security	Trust in security
	Digital literacy lacking	Need to keep up with tech Privacy protection requires knowledge
Platform concerns	Platforms and (dis)trust	Sneaky goals platforms Concerns location data
	Data sharing	Law enforcement use IPAs Data shared connected appliances
	Data use	Participating in A/B test Fear data profiling
	Consequences IPA data use	Household IPA makes lazy Remain autonomy

* From a total of 180 open codes

Appendix 15: Chapter 8 Codebook

Selective code	Axial code	Sample of open codes (verbatim)*
Media repertoires of interconnected families	Children's multi-device media use	Multi-tasking entertainment background Snapchat interacting with friends
	Parent's focused media use	Parents serious WhatsApp conversations Investigating new applications
	Digital family communication	Family WhatsApp group practical purpose Family WhatsApp group sharing pictures
	Resilience of children	Blocking unfamiliar friend/follower requests No sharing of personal details on TikTok
Ensuring openness & establishing rules	Open conversations media use	Consulting parent after incident WhatsApp Parents ask what child is streaming
	Family discussions digital risks	Social media risk bad intentions strangers Rules private account TikTok
Providing safety & guidance	Availability for safety	Location tracking for safety Child smartphone for biking to school
	Monitoring embedded in family life	Location tracking to locate parent Student tracking system check homework
	Tensions/ strategies monitoring	Snapchat to avoid monitoring Student tracking system experienced negative by child
Encouraging freedom & trust	No monitoring in parenting style	Location tracking unnecessary Freedom child important
	Trust in behaviour/ communication	Trust in good judgment social media Location communication based on trust

*From a total of 397 open codes

English summary

Privacy and surveillance have become everyday facts of life (Lyon, 2018). Both concepts are multidimensional and difficult to define. In this dissertation, I build on a social notion of privacy as something that facilitates social interactions, forms a social value, and plays a crucial role in social relationships and identity (Hughes, 2015; Regan, 2015; Steeves, 2009, 2015). Moreover, I connect this understanding of privacy to surveillance as a multidimensional concept. In our technology-saturated and interconnected world, people experience the effects of commercial, governmental, and interpersonal gathering, processing and sharing of personal data on a daily basis (Lyon, 2007; Marx, 2015a). However, mundane practices and considerations around privacy and surveillance are dealt with in an ambivalent way. For instance, people can be passionate about safeguarding their privacy and claim that they mitigate the influence of surveillance, yet still use certain social media and smart technologies that seemingly contradict these safeguards. This dissertation is predicated on the recognition that explanations of such contrasts as privacy paradoxes (Barnes, 2006; Brown, 2001) or privacy calculus (Bol, Dienlin, et al., 2018; Dinev & Hart, 2006) fail to grasp the multidimensional nature of privacy and surveillance experiences in everyday life.

Therefore, this dissertation studies everyday practices that surround the deployment of privacy preserving actions in relation to perceptions and experiences of surveillance. Through interviews and focus groups with 100 respondents, I explore how people use mobile and smart technologies on a daily basis. In order to understand their mundane experiences with privacy and surveillance, I focus on what people do rather than what their concerns are. This practice theory-oriented approach inspired by Reckwitz (2002), Schatzki (2005), and Shove et al. (2012) focuses on technology use as an assemblage of sociomaterial activities driven and motivated by particular knowledge, competences, and meanings. The empirical research in my dissertation is guided by the research question: **How do people experience privacy and surveillance in their everyday practices?**

To make sense of the accounts people provided of their privacy and surveillance mitigation practices in community, communicative, and inti-

mate contexts, I engaged in an inductive qualitative analysis of interview and focus group transcripts. More specifically, I followed a constructivist grounded theory methodology and approached the data in a bottom-up manner (Charmaz, 2014; Corbin & Strauss, 1990). In a three-phase analysis process, I first engaged in open coding in a verbatim style, after which I clustered the open codes in mutually exclusive sub-categories with a more conceptual character. Finally, these axial categories were connected to theoretical concepts and research questions to provide an in-depth understanding of the main overarching, recurring, themes in the interviews and focus groups. This dissertation includes six empirical studies each based on a separate constructivist grounded theory analysis.

The first part of this dissertation focuses on community contexts as a backdrop of privacy and surveillance experiences. I conducted interviews and focus groups with moderators and participants of WhatsApp Neighbourhood Crime Prevention (WNCP) groups. In WNCP WhatsApp group conversation, neighbours exchange warnings, concerns, and information about incidents, emergencies and (allegedly) suspicious situations related to their community. These exchanges often lead to citizens actively protecting and monitoring their streets, using camera-phones to record events or people they deem suspicious. WNCP groups are an important context for studying privacy and surveillance practices as they enable an examination of how community initiatives around safety have a direct impact on the neighbourhood dynamics and personal experiences of citizens. WNCP practices have ambivalent consequences for individuals and communities.

Chapter 3 highlights sociomaterial dimensions of WNCP practices and how these can be understood as a form of lateral, or interpersonal, surveillance (Andrejevic, 2002, 2007; Lee et al., 2017; Trottier, 2012). While voluntary citizen participation in crime prevention leads to an increase in social support, feelings of safety, and active prevention of break-ins, WNCP practices also default to neighbours monitoring each other. Such lateral surveillance practices can be seen to transcend digital monitoring and cause privacy infringement of neighbours and passers-by. Further, these practices create tensions between neighbours about correct safeguarding practices, potentially increase risky vigilant behaviour, and lead to a normalisation of distrusting attitudes.

In Chapter 4, I show how citizens make themselves responsible for policing their neighbourhood. The way in which they engage in participatory policing (Larsson, 2017; Reeves, 2012) does not follow guidelines as advised by the national Dutch police and likewise promoted by most WNCP moderators. Instead of informing the police and following their lead, citizens take up police work themselves. Their patrolling, monitoring, and prevention practices are problematic for several reasons. WNCP practices tend to increase distinctions between *insiders* and *outsiders*, normalise suspicion, challenge relations with the police, instigate illegitimate citizen actions, and potentially reinforce discriminatory practices. The research in Part 1 indicates that increased transparency is needed about how WNCP groups interact with more formal police structures, realistic guidelines should be designed and enforced, and purposeful trust building should be encouraged amongst neighbours and within neighbourhoods.

Part 2 presents digital communication as a context where people sculpt boundaries. Respondents actively manage boundaries between absence and presence, between different contexts, and around personal information. People engage in various digital conversations via WhatsApp and other platforms throughout the day. They are not only subjected to commercial surveillance by digital platforms, but also to lateral surveillance by their social contacts. However, attempts to ensure personal privacy protection through digital communication are constrained by social expectations that urge people to be continuously present, available, and responsive. Messaging apps such as WhatsApp as well as social media and other digital communication platforms collapse social contexts (Marwick & boyd, 2010; Vitak et al., 2012). Moreover, they also collapse the distinctions between digital and physical boundaries because people can be simultaneously present in digital and physical contexts (Pagh, 2020).

In Chapter 5. I explore how particular features of smartphones and messaging apps play a role in how individuals experience privacy. Respondents manage absence and presence with the help of WhatsApp functions to sculpt digital boundaries between different relational contexts including work, private life, and neighbourhoods. This chapter builds on research about negotiated networked absence (Burchell, 2017) and boundary theory (Nippert-Eng, 1996a, 1996b). Whereas existing research mainly focuses on the blurring of boundaries between work and private life, this study expands beyond the personal/professional binary and considers boundary work in more nuanced relational contexts. The findings from interviews with WNCP moderators and participants and employees of various workplaces highlight two forms of boundary work strategies. First, respondents purposefully tinker with WhatsApp features to manage the boundaries between absence and presence. Second, they use smartphone and WhatsApp functionalities to carefully construct segmentations between different contexts. The experience of being always available but always negotiating that availability affects everyday experiences of freedom, privacy, and autonomy in significant ways. Boundary sculpting practices around availability are defined by the meaning of particular contexts, the materiality of messaging apps, and technical know-how.

In Chapter 6, I focus on digital workplace communication to show how personal information disclosure and protection practices pose specific challenges for different professional groups. On the basis of interviews, I present communication privacy management (CPM) as a way that Dutch managers, office employees, self-employed professionals, and service industry employees manage boundaries around private information disclosure (Petronio, 2012). Their digital workplace communication can be characterised as dispersed given that it takes place via multiple devices and various platforms. Employees in different professional roles engage sociomaterial practices to manage the boundaries around their personal information. Managers protect their professional standing, office employees balance company culture against personal preferences, service industry employees anticipate boundary turbulence when social media and professional connections overlap, and self-employed professionals negotiate flexible and personal communication that proves to be paramount to their work. Chapter 6 adds to existing studies about CPM in work contexts (e.g., Frampton & Child, 2013; Laitinen & Sivunen, 2020) by expanding the scope from face-to-face or social media interactions to a collection of digital communication tools, differentiating between professional roles, and highlighting sociomaterial dimensions. The intangible nature of CPM practices instigates the need for employees to consider the risks of disclosing private information carefully. Moreover, employees and managers should actively engage with their colleagues, and professional relations to coordinate mutually understood privacy rules and employers need to be careful with information about their employees they receive via social media. The research in Part 2 shows how boundary and privacy management practices entail careful and ambivalent personal considerations.

I present two studies about different topics in Part 3 which are situated in the home. These studies view the home as an intimate context and revolve around issues of control within this space. The first study examines personal considerations around privacy and smart technologies that can be used to control the home whereas the latter study focuses on control over family members.

Chapter 7 studies Intelligent Personal Assistants (IPAs), also known as smart speakers, as novel interactive technologies with commercial surveillance capabilities that potentially infringe privacy expectations. Household IPAs are becoming part of everyday life in more and more households around the world and require connections to (social) media profiles, user accounts, and domestic appliances. Users can control their household with voice-activated commands to make life more convenient and efficient. Yet, IPAs also bring privacy and surveillance concerns about devices *listening in*, the *platformisation* of home life, and data security (Chandrasekaran et al., 2018; Liao et al., 2019; Lutz & Newlands, 2021). Chapter 7 combines a survey with qualitative focus groups among university personnel in order to provide an in-depth and multidimensional account of users' privacy concerns. Privacy concerns revolve around surveillance, security, and platform issues. The survey analysis indicates that platforms themselves are seen as a more important factor than the surveillance they may afford as is the security of the device more concerning than the surveillance it may afford. Moreover, the focus groups results revolve around conversation, recordability, locatability, control-ability, and assistance affordances and reveal that most respondents focus more on immediate and physical risks and have a pragmatic perspective towards hypothetical and long-lasting risks.

It becomes clear in Chapter 8 that the home also provides an intimate context for how early adolescents and parents exercise control over each other. In other words, this site is indicative of how they experience parental monitoring as a form of family surveillance. Parents can keep track of children's digital and non-digital activities and associations via digital technologies or more elementary solutions such as befriending their child on social media (Marsh et al., 2017; Marx & Steeves, 2010). Parental monitoring entails considerations of control, freedom, privacy, and care. As such, monitoring practices can lead to tensions and can restrain (early) adolescents in maintaining privacy, having autonomy, and developing their independence (Bennett et al., 2014; Nelson & Garey, 2009; Simpson, 2014). Based on interviews with early adolescents and parents, this study indicates how parents enforce screen time restriction practices, and use location tracking, digital monitoring tools, and student tracking systems. At the same time, insights are provided into how early adolescents reflect on and respond to such family surveillance practices. Their responses range from acceptance to resistance. Drawing on these findings, I indicate how family surveillance is embedded in broader constellations of media and communication practices and sometimes occurs in reciprocal ways. Open conversations about technology use are advised to foster privacy and cybersecurity resilience.

In answer to the research question, I conclude that people **experience privacy and surveillance through sociomaterial negotiations of appropriate forms of monitoring.** Privacy and surveillance negotiations are based on what people deem appropriate and inappropriate forms of monitoring. For instance, citizens might find it acceptable if neighbours monitor the street in front of their house but not if neighbours monitor when they are away. Such negotiations are sociomaterial because they are enacted through tangible elements like smartphones, social media interactions, and digital or physical conversations. Furthermore, negotiations of what people deem appropriate depend on the context. For instance, people experience parental monitoring in a different manner than commercial surveillance by household IPA platforms.

It is important to note that privacy and surveillance negotiations are constrained by inequalities and a lack of transparency. First, inequalities in decision making and digital literacy amplify or create power imbalances across contexts. Different levels of digital skills cause inequalities in privacy protection capabilities (for instance by muting a smart speaker) and in surveillance practices (e.g., engaging in interpersonal monitoring via WhatsApp's *blue checks* and *last seen* features). In addition, not everyone has the power to make decisions around privacy and surveillance (employees might for example be constrained in sculpting boundaries between personal and professional contexts when their supervisor messages them during the weekend). Second, a lack of transparency around commercial, lateral, and family surveillance practices leads to tensions and information imbalances. Based on these conclusions I suggest that open communication is crucial in increasing equality and transparency around interpersonal, family, and commercial surveillance. Moreover, tangibility is key to increasing awareness of and resilience in privacy and surveillance practices. Making complex surveillance issues and privacy solutions tangible via metaphors, examples, and visible markers, enables people to better identify surveillance practices and to apply privacy-preserving measures.

Nederlandse samenvatting

Alhoewel privacy en surveillance onderdeel uitmaken van ons dagelijks leven (Lyon, 2018), zijn dit complexe concepten die moeilijk te definiëren zijn. In dit proefschrift volg ik een sociale visie op privacy waarin privacy wordt gezien als een voorwaarde voor sociale interacties, sociale relaties en de ontwikkeling van identiteit (Hughes, 2015; Regan, 2015; Steeves, 2009, 2015). Een sociale visie op privacy is verbonden aan surveillance in verschillende vormen. Mensen ervaren surveillance wanneer persoonlijke informatie wordt verzameld, verwerkt en gedeeld voor commerciële, persoonlijke en overheidsdoeleinden (Lyon, 2007; Marx, 2015a). Mensen gaan hier in hun alledaagse doen en laten op een tegenstrijdige manier mee om. Ze kunnen bijvoorbeeld actief hun privacy beschermen door GPS op hun telefoon uit te schakelen maar tegelijkertijd slimme technologieën gebruiken die persoonlijke informatie verzamelen. Bekende theorieën verklaren de verschillen tussen overtuigingen en gedrag als een *privacy paradox* (Barnes, 2006; Brown, 2001) of *privacy calculus* (Bol, Dienlin, et al., 2018; Dinev & Hart, 2006). Deze verklaringen doen echter tekort aan de complexiteit waarop mensen privacy en surveillance ervaren.

Om die reden beschrijf ik in dit proefschrift hoe mensen in hun dagelijks leven gebruikmaken van mobiele en slimme technologieën in hun buurt, communicatie en huiselijke context. Dit proefschrift is gericht op het beantwoorden van de onderzoeksvraag: **Hoe ervaren mensen privacy en surveillance in hun dagelijks leven?** Mijn onderzoek is gebaseerd op interviews en focusgroepen met in totaal 100 respondenten over het gebruik van communicatieplatforms, toezichtsoftware en slimme technologieën. Deze benadering is geïnspireerd op *practice theory* (Reckwitz, 2002; Schatzki, 2005; Shove et al., 2012), waarin technologiegebruik wordt gezien als een activiteit met sociale en materiële componenten die worden gemotiveerd door kennis, competenties en bedoelingen.

Mijn onderzoeksresultaten zijn gebaseerd op kwalitatieve analyses van de interview- en focusgroeptranscripten. Deze analyses zijn geïnspireerd op *constructivist grounded theory*, waarbij analyses worden gestuurd door de data (Charmaz, 2014; Corbin & Strauss, 1990). In andere woorden, in plaats van te zoeken naar vooropgestelde thema's bekijk ik welke thema's er vanuit de interviews zelf naar boven kwamen. Deze aanpak verschaft inzicht in de overkoepelende gebruiken en percepties van technologieën. Dit proefschrift bevat zes hoofdstukken, elk gebaseerd op een afzonderlijke analyse.

Deel 1 omvat Hoofdstuk 3 en 4 en is gericht op de buurt als een context waarin mensen privacy en surveillance ervaren. Deze hoofdstukken zijn gebaseerd op interviews en focusgroepen met beheerders en deelnemers van WhatsApp Buurtpreventie (WABP) groepen. In WABP groepchats wisselen buren waarschuwingen, zorgen en informatie uit over incidenten, noodsituaties en (vermeende) verdachte situaties in de straat. Deze interacties leiden er vaak toe dat burgers hun straten actief beschermen en in de gaten houden, en de camera van hun mobiele telefoon gebruiken om gebeurtenissen of mensen die ze verdacht vinden vast te leggen. WABP-groepen vormen een belangrijke context voor het bestuderen van surveillanceactiviteiten omdat ze een directe impact hebben op de buurtdynamiek en de persoonlijke ervaringen en privacy van burgers.

Hoofdstuk 3 omschrijft hoe WABP-activiteiten zowel bestaan uit sociale factoren (mensen, interacties, normen) als materiële elementen (smartphones, straten, huizen, camera's). Ik toon aan hoe deze sociaal-materiële acties kunnen worden gezien als een vorm van *lateral surveillance* (Andrejevic, 2002, 2007; Lee et al., 2017; Trottier, 2012). Dit type surveillance duidt op interpersoonlijke vormen van monitoren waarbij mensen elkaar in de gaten houden. Hoewel vrijwillige burgerparticipatie in misdaadpreventie leidt tot een toename van sociale steun, gevoelens van veiligheid en actieve preventie van inbraken, hebben ze als bijwerking dat buren elkaar constant in de gaten houden. Deze interpersoonlijke surveillance overstijgt digitale controle en maakt inbreuk op de privacy van buren en voorbijgangers.

In Hoofdstuk 4 ligt de focus op hoe burgers zichzelf via WABP verantwoordelijk maken voor de veiligheid in hun wijk. Burgers nemen politiewerkzaamheden op zich, in andere woorden, ze doen aan *participatory policing* (Larsson, 2017; Reeves, 2012). In de praktijk volgen hun werkwijzen vaak niet de ideale situatie zoals voorgeschreven in de alomgebruikte SAAR-regels (deze afkorting staat voor *Signaleer, Alar-*

meer, App, Reageer, zie *Huisregels*, 2015). In plaats van eerst de politie te informeren en hun instructies te volgen, komen burgers direct zelf in actie. Zelfgeorganiseerde preventie-acties zijn om verschillende redenen problematisch: ze kunnen het onderscheid tussen *insiders* en *outsiders* vergroten, achterdocht normaliseren, relaties met de politie op scherp zetten, onwettige burgeracties stimuleren en mogelijk discriminerend gedrag veroorzaken. Het onderzoek in Deel 1 leidt tot de conclusies dat er meer transparantie nodig is over hoe WABP-groepen omgaan met formele politiestructuren, dat er realistische richtlijnen moeten worden ontworpen en gehandhaafd, en dat meer vertrouwen in buurten moet worden gestimuleerd.

Deel 2 presenteert digitale communicatie als een context waarin mensen grenzen afbakenen om hun privacy te waarborgen. Wanneer mensen gedurende de dag verschillende digitale gesprekken via WhatsApp en andere platforms voeren, worden ze niet alleen onderworpen aan commerciële surveillance, maar ook aan interpersoonlijke surveillance door hun sociale contacten. Mogelijkheden om privacy te beschermen in digitale communicatie worden echter beperkt door de sociale verwachting om continu digitaal aanwezig en beschikbaar te zijn. In digitale communicatieplatforms is het vaak lastig om onderscheid te maken tussen verschillende contexten. Dit veroorzaakt *context collapse,* oftewel het in elkaar overlopen van sociale contexten (Marwick & boyd, 2010; Vitak et al., 2012). Bovendien doet digitale communicatie ook het onderscheid tussen digitale en fysieke grenzen teniet, omdat mensen tegelijkertijd aanwezig kunnen zijn in digitale en fysieke contexten (Pagh, 2020).

In Hoofdstuk 5 onderzoek ik hoe bepaalde functies van smartphones en berichten-apps een rol spelen in hoe mensen privacy ervaren. Respondenten beheren afwezigheid en aanwezigheid en scheppen digitale grenzen tussen verschillende contexten. Dit hoofdstuk bouwt voort op onderzoek naar *negotiated networked absence* (het onderhandelen van afwezigheid terwijl mensen constant in contact staan, Burchell, 2017) en *boundary theory* (over het bewerkstelligen van sociale en fysieke grenzen rondom privacy, Nippert-Eng, 1996a). Waar bestaand onderzoek zich vooral richt op het vervagen van grenzen tussen werk en privé, omvat mijn onderzoek meerdere relationele contexten – zoals werk, privé, de buurt en hobby's. De interviews geven inzicht in twee vormen van *boundary work*. Ten eerste gebruiken mensen WhatsApp-functies (zoals de blauwe vinkjes) om de grenzen tussen afwezigheid en aanwezigheid te beheren. Ten tweede gebruiken ze smartphone-functies (zoals de *niet storen*-modus) om grenzen tussen verschillende contexten te bewerkstelligen.

Hoofdstuk 6 verschuift de focus naar digitale communicatie in de werkcontext, om te laten zien hoe mensen in verschillende beroepen omgaan met het delen en beschermen van persoonlijke informatie. Ik bouw voort op *communication privacy management theory* (Petronio, 2012) om te begrijpen hoe Nederlandse managers, kantoormedewerkers, zzp'ers en horecawerknemers de grenzen rondom privé-informatie beheren. Werknemers communiceren dagelijks via meerdere apparaten en verschillende platforms en lopen tegen functie-specifieke uitdagingen aan. Managers trachten hun professionele reputatie te beschermen in informele werkcommunicatie terwijl kantoormedewerkers een balans proberen te vinden tussen de bedrijfscultuur en hun persoonlijke voorkeuren. Horecamedewerkers ervaren dat een vermenging van hun persoonlijke en professionele context vanzelfsprekend lijkt in hun informele werkomgeving, maar tot frictie en dilemma's kan leiden wanneer ze sociale mediaconnecties onderhouden met collega's en klanten. Zelfstandige professionals ondervinden dat flexibele communicatie via persoonlijke kanalen van groot belang is voor hun werk. Het onderzoek in Deel 2 laat zien hoe het beheren van privacy ambivalente persoonlijke overwegingen met zich meebrengt.

In Deel 3 presenteer ik twee onderzoeken over privacy- en surveillance in en rondom het huis. In een huiselijke context oefenen mensen controle uit over apparaten via slimme technologieën (Hoofdstuk 7) en over gezinsleden met toegewijde software en digitale communicatie (Hoofdstuk 8). Hoofdstuk 7 bestudeert hoe interactieve digitale assistenten zoals Siri en Google Assistent in slimme speakers (*household intelligent personal assistants*) met commerciële surveillance inbreuk kunnen maken op privacy. Slimme speakers worden in steeds meer huishoudens wereldwijd onderdeel van het dagelijks leven en vereisen verbindingen met (sociale) mediaprofielen, gebruikersaccounts en huishoudelijke apparaten. Gebruikers kunnen hun huishouden besturen met spraakgestuurde opdrachten om het leven gemakkelijker en efficiënter te maken. Slimme speakers roepen echter ook zorgen op over privacy en digitale veiligheid met betrekking tot meeluisterende apparaten, de *platformisering* van het gezinsleven en beperkte digitale beveiliging (Chandrasekaran et al., 2018; Liao et al., 2019; Lutz & Newlands, 2021).

Aan de hand van een enquête en focusgroepen met universiteitspersoneel verschaf ik inzicht in de privacyzorgen van (toekomstige) gebruikers. Hun privacyzorgen zijn gericht op bewaking, beveiliging en digitale platforms. Uit de analyse van de enquête blijkt dat platforms zelf en digitale veiligheidsrisico's als zorgwekkender worden ervaren dan commerciële surveillance. De focusgroepen tonen aan dat privacyzorgen draaien om percepties van bepaalde functies (*affordances*) van slimme speakers, zoals conversatie, geluidsopnames, lokaliseerbaarheid, beheersbaarheid en assistentie. Bovendien laten de resultaten zien dat de meeste zorgen zich richten op directe en fysieke risico's: mensen maken zich meer zorgen over huisinbraken dan over digitale identiteitsdiefstal.

In Hoofdstuk 8 wordt duidelijk dat het huis de context vormt van hoe jonge adolescenten (10-15 jaar) en ouders elkaar in de gaten houden. Dit onderzoek bestudeert hoe ouderlijk toezicht wordt ervaren als een vorm van familiesurveillance. Ouders kunnen de digitale en niet-digitale activiteiten en connecties van kinderen volgen via toegewijde software of meer elementaire oplossingen zoals hun kind volgen op sociale media (Marsh et al., 2017). Ouderlijk toezicht draait om controle, vrijheid, privacy en zorg. Als zodanig kan het in de gaten houden van kinderen tot spanning leiden en adolescenten beperken in hun privacy, autonomie en (het ontwikkelen van) onafhankelijkheid (Bennett et al., 2014; Simpson, 2014).

Op basis van interviews met jonge adolescenten en ouders geef ik weer hoe ouders schermtijd beperken en gebruikmaken van locatietracking, digitale monitoringsoftware en leerlingvolgsystemen. Tegelijkertijd laat ik zien hoe jonge adolescenten reflecteren en reageren op familiesurveillance. Mijn onderzoek geeft weer hoe familiesurveillance is ingebed in dagelijks mediagebruik en dat surveillance soms een wederkerig karakter heeft. Open communicatie over technologie is van belang om mediawijsheid over privacy en digitale veiligheid te bevorderen.

In antwoord op de onderzoeksvraag concludeer ik dat **mensen privacy en surveillance ervaren in sociaal-materiële overwegingen over gepaste en ongepaste vormen van surveillance.** Mensen bepalen continu wat zij gepast en ongepast vinden en handelen daarnaar. Ze vinden het bijvoorbeeld wel gepast dat buren de straat voor hun huis in de gaten houden, maar niet dat buren bijhouden wanneer ze weg zijn. Dergelijke overwegingen zijn sociaal-materieel omdat tastbare elementen zoals smartphones, sociale media-interacties en digitale gesprekken hierin een rol spelen. Bovendien zijn dagelijkse overwegingen rondom privacy en surveillance afhankelijk van de context waarin ze plaatsvinden. Zo ervaren mensen het monitoren van kinderen bijvoorbeeld anders dan commerciële dataverzameling door slimme technologieën.

Onderhandelingen over privacy en surveillance worden beperkt door ongelijkheid en een gebrek aan transparantie. Allereerst bepalen ongelijke niveaus van digitale vaardigheden in hoeverre mensen hun privacy kunnen beschermen (bijvoorbeeld door een slimme speaker uit te zetten met de *mute*-knop) en surveillance kunnen uitvoeren en voorkomen (zoals via de *laatst gezien*-functie van WhatsApp). Bovendien heeft niet iedereen de mogelijkheid om beslissingen te nemen over zijn eigen privacy en surveillance (werknemers hebben bijvoorbeeld te maken met verwachtingen en ouders hebben meer zeggenschap over de privacy van hun kinderen dan andersom).

Ten tweede leidt een gebrek aan transparantie zowel op het vlak van interpersoonlijke en familie- als commerciële surveillance tot spanningen en informatie-ongelijkheid. Op basis van deze conclusies benadruk ik dat open communicatie over al deze vormen van surveillance cruciaal is voor het vergroten van gelijkheid en transparantie. Tot slot is tastbaarheid de sleutel tot het vergroten van bewustzijn over privacy en surveillance: Door complexe surveillancevraagstukken en privacyoplossingen tastbaar te maken aan de hand van metaforen, voorbeelden en zichtbare risico's, kunnen mensen surveillancepraktijken beter identificeren en privacybeschermende maatregelen toepassen.

Portfolio

List of publications related to PhD project

Academic publications

Mols, A. (under revision for first round of R&R at the time of printing) “Even jokes are work-related”: Sociomaterial communication privacy management practices. *Information, Technology & People*

Mols, A., Wang, Y. & Pridmore, J.H. (accepted for publication). Household Intelligent Personal Assistants in the Netherlands: Exploring Privacy Concerns around Surveillance, Security and Platforms. *Convergence*

Mols, A. (2021). Digital literacy and information inequality in Dutch WhatsApp Neighbourhood Crime Prevention groups. *Criminological Encounters, 4*(1), 223-227. https://doi.org/ 10.26395/CE21040119

Mols, A. (2021). Citizen Participation in Community Surveillance: Mapping the Dynamics of WhatsApp Neighbourhood Crime Prevention Practices. In H. Rahman (Ed.), *Human-Computer Interaction and Technology Integration in Modern Society* (pp. 157–176). https://doi.org/10.4018/978-1-7998-5849-2.ch007

Mols, A., & Pridmore, J. (2020). Always available via WhatsApp: Mapping everyday boundary work practices and privacy negotiations. *Mobile Media & Communication,* 1–19. https://doi.org/10.1177/ 2050157920970582 (Shortlisted for *EGSH PhD Excellence Best Article Award 2020)*

Mols, A., & Pridmore, J. (2019). When Citizens Are “Actually Doing Police Work”: The Blurring of Boundaries in WhatsApp Neighbourhood Crime Prevention Groups in The Netherlands. *Surveillance & Society, 17*(3/4), 272–287. https://doi.org/10.24908/ss.v17i3/4.8664

Co-authored articles

Pridmore, J., & Mols, A. (2020). Personal choices and situated data: Privacy negotiations and the acceptance of household Intelligent Personal Assistants. Big Data & Society, 7(1), 2053951719891748. https://doi.org/10.1177/2053951719891748

Pridmore, J., Zimmer, M., Vitak, J., Mols, A., Trottier, D., Kumar, P. C., & Liao, Y. (2019). Intelligent Personal Assistants and the Intercultural Negotiations of Dataveillance in Platformed Households. Surveillance & Society, 17(1/2), 125–131. https://doi.org/10.24908/ss.v17i1/2.12936

Pridmore, J., Mols, A., Wang, Y., & Holleman, F. (2018). Keeping an eye on the neighbours: Police, citizens, and communication within mobile neighbourhood crime prevention groups. The Police Journal: Theory, Practice and Principles, 92(2), 97–120. https://doi.org/10.1177/0032258X18768397

Non-academic publications

Mols, A. (2018). Interacting with a smart speaker [blog post]. *PhD club blog.* https://www.eur.nl/en/eshcc/news/interacting-smart-speaker

Mols, A. (2017). Attentie! WhatsApp buurtpreventie: een verkenning van een ambivalent fenomeen. *P&I Privacy en Informatie, 5*, 211.

Conference presentations related to PhD project

Mols, A. & Pridmore, J.H. (2021, October 6). Negotiations around Digital Wellbeing in Networked Families. *4S Annual meeting. Good Relations, Practices and Methods in Unequal and Uncertain Worlds.* Virtual Conference.

Mols, A., Wang, Y. & Pridmore, J.H. (2021, September 8). “OK, Google, make me coffee”: Trust and privacy attitudes towards interacting with Intelligent Personal Assistants and smart speakers in the Netherlands. *8th ECREA European Communication Conference.* Virtual Conference

Liao, Y., Mols, A., Vitak, J., Zimmer, M., Trottier, D., Kumar, P., & Pridmore, J. (2020, May 21). When Does Data Collection and Use Become a Matter of Concern? A Cross Cultural Comparison of American and Dutch People’s Privacy Attitudes. *ICA 2020 - 70th Annual ICA Conference*. Virtual Conference

Pridmore, J., & Mols, A. (2019, May 24). “Hey, Why Didn’t You Respond?” Mobile Messaging and Everyday Boundary Work Practices. *ICA 2019 - 69th Annual ICA Conference*. Washington, D.C., United States

Mols, A. (2019, October 14). “Work and personal life, they just blur together” Messaging apps and the amplification of workplace surveillance and context collapse. *ICSI 2019: (Re-)Connecting Perspectives on Interpersonal Communication & Social Interaction.* Tilburg University, The Netherlands.

Mols, A. (2018, October 5). Checking my messages and myself: Privacy negotiations, management strategies and everyday practices in the use of messaging apps. *Amsterdam Privacy Conference.* Amsterdam, The Netherlands

Mols, A. & Pridmore, J.H. (2018, June 9). "Work and personal life, they just blur together" Messaging apps and the amplification of workplace surveillance and context collapse. *Surveillance Studies Network 8th Biennial Conference*: Aarhus, Denmark

Mols, A. & Pridmore, J.H. (2017, September 1). Citizens, safety and the precariousness of digital community initiatives. *4S 2017 STS (In)Sensibilities*: Boston, United States

Mols, A., Pridmore, J.H. & Trottier, D. (2017, May 19). Watching our neighbours: The negotiation of privacy in neighbourhoods. *TILTing Perspectives.* Tilburg University, The Netherlands

Guest and invited lectures

2021 *Negotiating presence, boundaries, and romantic relationships.* Technology, Media and Identity [International Bachelor Communication and Media], Erasmus University Rotterdam, the Netherlands

2019 *When citizens are "actually doing police work".* Smart Cities Chair Master Class Hyperlocal Networks and Initiatives, Vrije Universiteit Brussels, Belgium

2018 *Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems: Practices and Contexts in the Netherlands and US.* Roundtable: Smartphone ecosystems, *Amsterdam Privacy Conference*, the Netherlands

2018 *Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems: Context & Practices in the Netherlands & US.* PRICE EAGER Workshop Cyber Security Research, The Hague, the Netherlands

2017 *Consumer Surveillance in a Platform Society* (w/Jason Pridmore). Privacy, Surveillance and New Media Technologies [International Bachelor Communication and Media], Erasmus University Rotterdam, the Netherlands

2017 *Materialised (dis)trust: Mapping the dynamics of WhatsApp neighbourhood watchfulness practices.* Surveillance Studies Centre Research Seminar, Queens University Kingston, Canada.

Media appearances

2019, Dec 2	Doorbell Cameras Are Popular, But Should We Be Sharing The Videos Online? [radio interview]. *NPR All Things Considered.* https://www.npr.org/2019/12/02/784225316/doorbell-cameras-are-popular-but-should-we-be-sharing-the-videos-online?t=1618304435365
2018, Dec 12	Hoe kunnen we slim omgaan met smart speakers? [Video interview] *Erasmus University Rotterdam*. https://www.eur.nl/nieuws/hoe-kunnen-we-slim-omgaan-met-smart-speakers
2018, Oct 30	Wie is er bang voor Google Home? [Interview] *Erasmus University Rotterdam.* https://www.eur.nl/nieuws/wie-er-bang-voor-google-home
2018, Dec 17	Spitsuur [radio-interview]. *BNR Nieuwsradio Tech Update*. https://www.bnr.nl/player/archief/20181217164100300

Academic services

2019-2022	Co-organizer Surveillance Studies Network Conference, Erasmus University Rotterdam
2020	Jury member NeFCA 2019 Dissertation Award
2017-2021	Management ERMeCC Research Lab
2018/2019	Chair ERMeCC PhD Club
2017/2018	Vice-chair ERMeCC PhD Club
2016-2021	Peer reviews for *International Journal of Communication, Surveillance & Society, New Media & Society* and *Cyberpsychology*

Courses and training followed during PhD project

Academic/Methodological:

2021	*Communicating your research: Lessons from Bitescience*, EGSH, Erasmus University Rotterdam, virtual meetings
	RMeS Winterschool and Graduate Symposium, virtual meetings
2018	*RMeS Winterschool and Graduate Symposium*, University of Amsterdam, the Netherlands
	Professionalism and integrity in research, EGSH, Erasmus University

Rotterdam, the Netherlands

2017 *RMeS Winterschool and Graduate Symposium*, Erasmus University Rotterdam, the Netherlands

Hendrik Muller Zomer Seminar, Koninklijke Nederlandse Academie voor de Wetenschappen (KNAW), Amsterdam, the Netherlands

Surveillance Studies Summer Seminar, Surveillance Studies Centre, Queens University, Kinston, Canada

'How Do You… Communicate to a General Public?" RMeS Network Event, Utrecht, the Netherlands

2016 *Brush up your SPSS skills*, EGSH, Erasmus University Rotterdam, the Netherlands

Advanced research methods 1: qualitative data analysis, EGSH, Erasmus University Rotterdam, the Netherlands

Self-presentation: presenting yourself and your research, EGSH, Erasmus University Rotterdam, the Netherlands

Making an academic poster that stands out, EGSH, Erasmus University Rotterdam, the Netherlands

Didactic training

2016 *Basic didactics course* (Research Training Consultancy RISBO)

Courses taught during PhD project

MA thesis supervision Media and Business MA

Bachelor thesis class / BA-3 thesis supervision International Bachelor Media and Communication

Internship supervision BA-2/3

Workshop: Academic Skills BA-1

Media and Communication Theory Pre-master/BA-2/Minor

New Media and International Business BA-2

Research Workshop: Cross-national Comparative Research BA-1

Media Processes and Influences BA-1

Key Concepts in the Social Sciences BA-1

Communication as a Social Force BA-1

Communication and Media Labour Market Orientation BA-2

EVERYDAY EXPERIENCES OF PRIVACY AND SURVEILLANCE

BY ANOUK MOLS

Privacy and surveillance are embedded in everyday life. This dissertation explores the mundane technology use of 100 respondents in community, communicative, and intimate contexts. The results show that they experience privacy and surveillance through sociomaterial negotiations. People negotiate what forms of interpersonal, family, and commercial surveillance they deem (in)appropriate and respond accordingly. These personal considerations are influenced by the context, the technologies involved, knowledgeability and (in)equality, and the transparency of monitoring practices.