KATARINA WINTER & KLARA HERMANSSON

(Dis)affordances and abandonment

Understanding everyday user engagement with security apps

Abstract
In recent decades, numerous security technologies have emerged with the aim of fostering secure communities and providing people with the tools to bolster their everyday safety. Focusing specifically on security apps, this article explores how apps addressing security in public and semi-public spaces constitute preconditions for everyday user engagement, and vice versa, how users actively respond to these preconditions. Through identifying the (dis)affordances involved in such processes, we investigate co-production of user engagement with security apps. Drawing on observations and interviews with producers and users of apps, we explore the landscape of security apps as pervaded by processes of intended and actual (dis)affordances, sometimes also leading to abandonment of both use and users. A key finding is the divergence between the intended purposes of these apps – often framed around broad security ambitions – and their actual use, which frequently intertwines with mundane routines and logistical needs. This divergence paradoxically legitimizes broader securitisation discourses, even as the apps' "successful use" often reflects a relatively privileged everyday life distant from tangible threats, highlighting the complex interplay between market forces, user practices, and the normalisation of surveillance.

Keywords: Security technologies, mobile applications, (dis)affordances, user engagement, securitisation

THE PRESENT ARTICLE examines mobile applications as a case study of security technologies aimed at enhancing everyday public safety. Along with a development where digitalisation has increasingly influenced various aspects of welfare (Andreassen, Kaun & Nikunen 2021), the notions of safety and security[1] have evolved, shifting emphasis from conventional welfare issues to concerns related to (fear of) crime (Hermansson 2018; Sahlin Lilja 2018; Stanko 2000). Numerous security technologies, ranging from CCTV to sensors and mobile applications (hereafter apps) have emerged to foster secure communities and provide societies and individuals with the tools to bolster everyday security. At least that is how such technologies are introduced to their potential users in the increasingly growing security market. Focusing specifically on apps, this study explores how apps addressing security in public and semi-public spaces create

1 The Swedish concept of "trygghet" encompasses both safety and security, while its counterpart "otrygghet" (insecurity) refers to people's fear of crime, general insecurities, and the material risk of being subjected to crime. In this article, safety and security are used interchangeably.

https://doi.org/10.37062/sf.62.27825
Sociologisk Forskning, årgång 62, nr 1–2, s. 59–84.

preconditions for user engagement, and, conversely, how users actively respond to these preconditions.

Apps are entrenched in our mundane routines and everyday life (Morris & Elkins 2015; Dieter et al. 2018), and scholars have engaged in app studies on various topics, such as health, shopping, and dating. However, security's broader and more nuanced societal implications remain understudied from perspectives involving apps (Wood, Ross & Johns 2022: 1093). These implications include increased societal insecurity due to technological changes (Zuboff 2019), security's role in contemporary responsibility (White & McMillan 2020) or inequality perspectives (Costanza-Chock 2020) and shifts in mundane communication patterns (Ling & Lai 2016). This gap can partly be explained by the slow appification of crime prevention, "the creation of apps designed to prevent crime through a variety of measures", which has primarily focused on law enforcement, surveillance, and correctional treatment (Wood, Ross & Johns 2022: 1094).

Empirical insights into the everyday routines of security apps can contribute to understanding how societal and political shifts brought about by digitalisation and the expansion of securitisation (Neocleous 2008; Ferguson 2017) intersect with everyday life. The 11 September 2001 attacks marked a significant turning point in global security policies, making threat discourses central in international relations. By framing discourses as existential threats, extraordinary measures such as new laws and policies that prioritise security over other societal needs are justified. This article provides an analysis of some of the often-neglected everyday technologies that emanate from such expansion of securitisation, specifically focusing on security apps.

Acknowledging the call to "move from content to practices" (Dieter et al. 2018: 13), we examine how apps addressing security in public and semi-public spaces interact with everyday activities. This approach necessitates sensitivity to the complexities of user engagement, not only because much happens between producers and users of apps, but also because users actively engage with apps in diverse ways. We combine the concept of (dis)affordances (Costanza-Chock 2020) – the possibilities and hindrances for engagement that apps offer their users – with an approach that considers users' active and mundane (e.g. practical and emotional) use to explore how they collectively participate in co-producing user engagement.

Security apps in context

International research has identified the increased importance attached to security and fear of crime in western criminal policy in recent decades (Stanko 2000; Bauman 2006; Hermansson 2023). When "fear of crime" first emerged as a public and political concern in the 1980s, it was understood as being closely connected to the risk of victimisation (Garland 2001). Today, insecurity and fear of crime have been established as concerns in their own right (Young 1996; Hermansson 2018). Through the discourse on insecurity, we are all constituted as "potential fearers" according to Young (1996), and crime becomes a problem concerning us all (Andersson 2010; Hermansson 2018).

The normalisation of (in)security as an everyday local and global concern has been discussed by various scholars in securitisation, surveillance, and policing studies (e.g. Hope & Sparks 2000; Massumi 2005; Franko, Gundhus & Lomell 2008; Low 2008; Fawaz & Bou Akar 2012; Fassin 2014; Riddell 2023). This normalisation legitimises the expansion of control in general, and digital technologies in particular, to protect the public (e.g. Maguire, Frois, & Zurawski 2014; Masco 2014). Scholars have raised concerns about how securitisation can be counterproductive, leading to increased feelings of insecurity (Flyghed & Hörnqvist 2003; Low 2008), and moreover, how responsibility for crime prevention has become individualised as well as privatised (Garland 2001; Aas 2006; Winter 2025).

Security apps lie at the intersection of these processes. Their societal establishment can be viewed as a manifestation of responsibilisation processes, where private companies actively seek to participate in (and position themselves as solutions to) crime prevention and safety enhancement. Simultaneously, the use of apps could potentially reinforce the individualisation and privatisation of responsibility for crime prevention, shifting focus from collective, societal approaches to personal, smartphone-based initiatives.

Researchers have examined mobile apps and their social implications across various disciplines, including Criminology, Sociology, Science and Technology Studies (STS), and Critical Data Studies. While security aspects have received some attention, much of the research has focused on apps in other areas of life. As apps constitute a significant part of contemporary everyday life, user perspectives have been explored in studies of health (e.g. Pink et al. 2017; Lupton 2012; 2014) and dating-related (see, e.g. McVeigh-Schultz & Baym 2015; Broeker 2023) apps. Continuing on user perspectives, research has also investigated users in algorithmic imaginaries (Bucher 2016), users' understanding of data collection and datafication (Lai & Flensburg 2020b), discrepancies between users' opinions and actions (Barth & de Jong 2017), new coalitions such as the "produser", "prosumer", and "produsage" (Michael & Lupton 2016), and how users become commodified through app data production and use in commercial as well as functional ways (Flensburg & Lai 2022).

App studies using a CDS approach have mainly emphasised perspectives on data, ownership, and privacy. Studies have, for example, examined the surveillance ecology and infrastructures involved in communication control, collection and distribution of data through apps, and how market actors navigate power (Lai & Flensburg 2020a, 2020b; Flensburg & Lai 2022).

Studies on apps in relation to security and crime prevention reflect the public debate on how new technologies, in general, often present a polarised view, either celebrating techno-utopian success or highlighting failures and risks (Costanza-Chock 2020). While some studies emphasise crime preventive apps' various functions and potential (Cumiskey & Brewster 2012; Chand et al. 2015; Viswanath & Basu 2015), others warn about risks associated with the use of new digital tools. Such risks relate to, for example, increased vulnerability (Wood, Ross & Johns 2022), undermining of victims of crime (White & McMillan 2020), or exacerbation of racism and structural violence

(Kennedy & Coelho 2022). Research has shown that apps can create an illusion of control (Maxwell et al. 2020; Kettrey et al. 2024) and reproduction of fear (Simpson 2014). Other risks include negative consequences for tracked children (Malone 2007; Oostveen et al. 2014; Simpson 2014) and increased possibilities for stalking (Fraser et al. 2010; Chatterjee et al. 2018; Messing et al. 2020). Studies have also explored tensions between "good" and "bad" effects, for example, discussing how apps bring both safety and anxiety, surveillance (surveillance from above) and sousveillance (surveillance from below) (Riddel 2023), how responsibilisation is transcoded into the apps themselves (Wood, Ross & Johns 2022: 1105), and that users in high income areas are more likely to use these apps (Ceccato 2019). In addition, although not a phenomenon exclusive to security apps, societal enthusiasm over apps as exemplified by media and political narratives is hardly supported by research or evaluation. Apps lack evidence; systematic evaluations of crime prevention apps or studies on their efficacy in reducing victimisation are rare (Wood, Ross & Johns 2022, their evaluation is an exception).

Security apps in relation to user perspectives are particularly understudied. Given the ethical complexities surrounding security technologies and app use (e.g. data collection on citizens, location-sharing and tracking, normalisation of surveillance, etc.), and moreover, that security apps are both broadly and specifically motivated by arguments on public engagement for public safety, it is crucial to increase knowledge on users of security apps and how their engagement intersects with broader social processes. For example, security apps bring new and old actors and interests for public engagement and responsibilisation. In relation to this, existing studies have emphasised the need to scrutinise how neoliberal rhetoric of empowerment and self-reliance is reinforced through digital security consumption, promoting new forms of public engagement tailored to markets and private interests rather than to the needs of individual citizens (Kennedy & Coelho 2022).

Previous research has stressed the need to explore mundane data – data generated in everyday situations without people noticing or acknowledging – to theorise change and to contextualise the massive amount of digital data used to explain and predict future developments in contemporary society (Pink et al. 2017). We explore users' everyday routines with apps as a meaning-making enterprise that legitimises the continuous generating of mundane data. Users are engaged both as producers of and content in data through their everyday use of mobiles (Michael & Lupton 2016), and they are ascribed responsibilities for their own and others' security. Apps reshape the landscape of public engagement, presenting both hindrances and opportunities in addressing new and old societal problems either as caring and responsible citizens or as potential victims of crime.

Methodological-analytical framework

To comprehend user engagement with security apps, it is crucial to consider both producers[2] and users (Bucchi & Trench 2014). This study draws on a broad empirical base, combining an overview of the security app field with interviews with and observations of both producers and users.

Data collection spanned from spring 2023 to spring 2024. Initially, we mapped all available apps, documenting how purposes, functions, users, and use were formulated within each initiative. This mapping, continuously updated, currently includes 48 apps. Case studies involving interviews and observations were selected, drawing inspiration from Wood, Ross & Johns's (2022) evaluation of crime prevention apps. While their identification of six app types – self-surveillance apps, decision aid apps, child-tracking apps, educational apps, crime-mapping/alert apps, and crime reporting apps – is largely mirrored by our mapping, Swedish apps tend to be more hybrid, often combining multiple functions. For instance, apps include alerting *and* reporting, or self-surveillance *and* child tracking. The apps are often initiated by coalitions of different private and public actors such as influencers, entrepreneurs, academics, and professionals/practitioners.

We analysed app descriptions user reviews from app stores and additional material from web pages and advertising campaigns (information on products, publicly available interviews with company CEO's as well as users, etc.). Two overarching framings emerged: *increased security* and *community building for prevention and safety*. Through our mapping, five primary app functions were identified: obtaining information, enabling communication (with specific community members or users in general), alerting (community, alarm central or private guards), sharing data/location, and reporting (crime, and/or activities of in/securities). Three broader user categories were found: apps for the general public, for organisations responsible for public safety (e.g. schools, municipalities, universities, etc.), and for specific publics (e.g. parents, neighbourhood specific users). We selected one case from each category for detailed analysis.

Producers were contacted via email, while users were reached through official contacts (such as school principals) and thereafter snowballing, or through social media calls. Interviews were conducted through individual physical meetings (three producer interviews and six user interviews), digital individual interviews (ten user interviews), and physical participant observations (two full-day workshop observations). Producer interviews focused on app framings and expectations, while user interviews explored everyday processes related to app use (or lack of use). All interviewees were pseudonymised and quotes were translated from Swedish to English, preserving original meanings as closely as possible.

The material was coded using Nvivo software. We applied an open coding strategy

2 While it is also important who gets to develop apps, we are here focusing on who gets to use them, and how. Therefore, producers are examined only in the way they create preconditions for user engagement.

inspired by Charmaz's (2006) grounded theory approach, initially treating each case as a separate unit to identify similarities and differences. Subsequently, focused coding grouped codes based on intended and actual use. This process identified variations, contradictions, and coherence in how apps, use, and users were ascribed to and infused in overarching discourses and practices of security on the one hand and everyday life on the other. This work was iterative, maintaining focus on empirical data while remaining sensitive to potential theoretical insights.

To analyse the forms of use that apps require and/or provide, we employed the concept of (dis)affordances. Affordances is a widely used notion of "action possibilities" (Gibson 1966, 1979). Later introduced to various fields including Design Studies (Norman 1988), Sociology, and Science and Technology Studies (STS) (Hutchby 2001) this concept has sparked various debates regarding its relevance and usefulness (see e.g. Woolgar 2002; Hutchby 2003; Rappert 2003; Bloomfield, Latham & Vurdubakis 2010).[3] Our approach draws on two key claims acknowledging the complexity of this debate.

Firstly, engaging with affordances necessitates exploring not only *what* an affordance is, but also *when*, for *whom* (Engestrom 1990; Bloomfield, Latham & Vurdubakis 2010), and, we argue, *where* it occurs. This aligns with Costanza-Chock's (2020) emphasis on examining affordances from perspectives of inequalities in availability and perceptibility. Costanza-Chock (2020) illustrates how technological objects, through their disaffordances, can reproduce inequalities and lead to exclusion, even when inclusionary intentions exist. This occurs because structures are hard-coded into technologies through unintentional mechanisms such as assumptions about end users and biases in data sets.[4] Consequently, we attend to the intended and actual use and users of these apps, as well as the temporal and spatial context in which they operate.

Secondly, we approach affordances as a subject for analysis rather than explanation (Rappert 2003), engaging with affordances as a process of co-production between ac-

3 Affordances is a concept coined by American psychologist James Gibson (1966, 1979) and early adopted and further introduced by design scholar Donald Norman (1988) and others to explain "the characteristics or properties of an object that suggest how it can be used. It shows a user that an object can be interacted with" (Interaction Design Foundation 2024). Since its introduction into Sociology and Science and Technology Studies (STS) by Ian Hutchby (2001) as well as its significant impact and/or transition into other fields, it has been a concept of dispute (see e.g. Woolgar 2002; Hutchby 2003; Rappert 2003; Bloomfield, Latham and Vurdubakis 2010). Whether the use of affordances can solve the determinism/constructivism divide in STS (Hutchby 2001) is not our focus here. We are also humbly aware of the potentials of other closely related concepts such as scripts (Akrich and Latour 1992). Our analysis was primarily empirically grounded, and Costanza-Chock's (2020) approach on (dis)affordances turned out to be particularly useful for attending to the empirical insights made, especially regarding the inequalities built into the expectations and practices of security app use.

4 According to Costanza-Chock (2020: 57), researchers must "denormalize the universal user" and engage with how "design reproduces a matrix of domination". The matrix of domination (originally a term from sociologist Patricia Hill Collins) refers to race, class and gender as intersecting systems of oppression, and is thereby linked to intersectionality. Such structures are "hard-coded into designed objects and systems" because of unintentional mechanisms such as assumptions about end users and bias in data sets. Although we do not engage fully with the domination matrix concept, it is indeed useful to illuminate what kind of user that the apps are encouraging and intending.

tors, discourses and practices. This approach recognises the interplay between intended and actual everyday app use. Following Michael (2000), we view affordances, users, and use as *co-present* with other people, objects, discourses, spaces, and temporalities. As argued by Bloomfield, Latham & Vurdubakis (2010: 428), affordances can be "catalysed by or interfered with" by co-presence. For instance, the co-presence of different temporalities – such as potential future threats perceived as rational concerns to address in the present, or future intentions to discontinue app usage (e.g. ceasing to track a child as they enter adolescence and require more privacy) – effectively legitimises the app's use, thereby catalysing its affordances.

Costanza-Chock differentiates between disaffordances – actively blocking certain users from use (e.g. stairs preventing wheelchair users from entering a building) – and dysaffordances – allowing use but forcing users into discriminating compromises (e.g. binary choices for non-binary individuals). While these examples illuminate inequalities related to affordances, our analysis reveals examples that exist between the "dis" and "dys" of affordances. For the sake of simplicity, we will use the term "disaffordances" throughout the study. Furthermore, to emphasise the co-producing aspects of "non-use", we introduce the concept of abandonment. While disaffordances refer to processes stemming from the apps or their producers, processes of abandonment may originate from users themselves or from inherent disaffordances within the technologies.

This framework allows for a comprehensive examination of security apps, exploring how they create preconditions for user engagement and how users respond to these preconditions. It considers engagement as an act of co-production of producer intentions and user experiences within the broader contexts of security discourses and everyday practices.

Results

This article addresses user engagement as processes of co-production, where producers of security apps frame their initiatives and create preconditions for user engagement, and users actively respond to these preconditions. Both producers' intentions and users' actual engagement with security apps are ongoing negotiations, produced at the intersection of discourses and practices associated with the apps. We analyse affordances as well as disaffordances associated with the apps in relation to both producers and users.

Intended affordances: Producers' perspectives

The framing of security apps, as found in marketing campaigns, news articles, and app store descriptions, draws on overarching securitisation discourses. These portrayals depict a negative societal development concerning crime and (in)security, coupled with solutions offered by the app. While the "security" addressed by these apps is broad in scope, the problems they target are often narrower, frequently linked to threats of violence in public spaces and perceived dangers of the stranger or unknown. The following quotation from a security app company's web page, illustrates this framing as the producer positions their initiative in the context of a society described as increasingly unsafe:

> Safety for everyone. Society has changed. Today, 28% of all Swedes between 18-65 years old feel unsafe in their own residential areas, and we want to change that. We are a security-enhancing company with a mission – to make people feel safer. Our first initiative has been to develop a service that most people can afford. We are Sweden's first mobile alarm. If you feel unsafe, just release the button and we'll send a security guard to your location. (Producer N, security app directed to the public)

The statement reflects a negative societal narrative about increased insecurity among Swedes and highlights the need for reliable solutions to address this issue. The company positions itself as a security-enhancing entity striving to make people feel safer while promising "safety for everyone" and affordability for "most people" to act to enhance their safety. Several apps employ similar rhetoric regarding an increasingly unsafe society, addressing insecurities related to walking home late at night or rising incidents of lethal violence. Although the target groups for these apps may differ, there is a consistent focus on securing oneself and others, while presenting the apps as reliable solutions to imagined threats.

To further understand the intended use and users of security apps, we examine their built-in functions. As touched upon above, common functions include alerting and reporting. Other main functions are communication tools, data sharing, location tracking capabilities, and obtainment of information. Thus, intended users are conceptualised as individuals who need or desire these functions – those seeking alarm capabilities, wanting to communicate with other users or specific community members, seeking to report activities, obtain information, or having needs related to the possibility of sharing their location.

While various uses for these functions can be envisioned, they often reflect singular and homogenous problems and possibilities. For instance, accurate information combined with efficient communication is fundamental to many apps. The apps claim to provide users with insights related to crime and security. However, as mentioned earlier, this information predominantly pertains to public spaces – how safe individuals perceive different areas, the inconveniences associated with these spaces, as well as to be informed by others or by the app about such activities in public space. Additionally, these apps aim to facilitate effective communication among community members to enhance overall feelings of security and establish efficient communication routes during emergencies and threats. While these motives appear broad and flexible at first glance, communication, as well as the other functions, are secondary to, and serve, an overarching security logic:

> In recent years, Sweden and other European countries have witnessed a troubling increase in school attacks and critical incidents, underscoring the urgent need for reliable school safety solutions. Schools must be prepared to respond rapidly — communicate effectively and ensure compliance with established action plans for any emergency or everyday incident. (Producer K, security app for organisations and workplaces)

This quote from an app's promotional material exemplifies the typical framing of security apps discussed earlier, specifically regarding communication functions. Intended affordances are framed as conditional upon perceived security threats such as school attacks. The recurrent reinforcement of stereotypical fear scenarios alongside enthusiasm for app features designed to mitigate such security concerns is prevalent throughout the material. Alternating between micro and macro, the big and the small, the dramatic threats of terror attacks and the everyday insecurities related to our neighbourhoods might suggest broad affordances. However, these seemingly separate aspects of security technologies are deliberately intertwined, or, in Michael's (2000) words, co-present. Although we may not consciously acknowledge all these aspects, rejecting tools purportedly designed to protect our loved ones, colleagues, students, or those under our care, requires considerable confidence. Apps operationalise moral imperatives around security by transforming responsibilities for our own or our peers' safety into practices like location sharing and various forms of communication. For instance, child tracking apps often emphasise features like geolocation to reassure parents about their children's safety:

> Our parental app gives you full control, and you receive immediate notifications about your child's activities and location. Create "safe zones" for added security and peace of mind. (Producer M, security app for parents and children)

The affordances embedded in these apps tie users' moral obligations to control over their children's security. Securitisation discourses are thus challenging for most individuals to resist since they resonate with core societal values. This normalisation of fear of crime positions users in a perpetual state of vulnerability or potential victimhood – a state often associated with passivity (Hermansson 2018). However, in this context, vulnerability manifests as an obligatory claim regarding users' roles in approving these narratives, thereby evolving into active engagement.

This shift from passive vulnerability to active engagement aligns closely with the principles of situational crime prevention. Situational crime prevention emphasises reducing criminal opportunities by altering the immediate environment in which crimes occur and empowering individuals and communities. Security apps manifest this approach by enabling users to actively engage in their own and their communities' safety. The apps thereby transform everyday realities and individuals into agents of crime prevention and security enhancement. Society – particularly in public spaces – is portrayed as a reservoir of suspicious activities and people, yet there exists hope. If users are sufficiently encouraged to utilise the apps, they can contribute positively towards creating safer communities. For instance, functions such as alert security guards or peers, or reporting inadequate lighting or "unsafe activities" in public spaces aim to address public space deficiencies.

Notably, one app initiative with the explicit aim of fostering community and sustainability differs from typical securitisation discourses. While it shares functions with other security apps and acknowledges and shares the idea (and the delimitation) that

public space has the prioritised potential to influence our sense of security, its framing is more positive, encouraging users to report "safe" rather than unsafe activities.

The formulation of expected needs, users, and usage remains an ongoing process. Producers' initial ambitions might prove difficult or unrealistic to attain over time. Producers either choose or find themselves compelled to abandon initial ideas and target groups. The establishment of security apps depends on market dynamics, where demand – and potential profitability – shapes how successfully an app can thrive. In light of such factors surrounding demand and profit margins, producers may reframe their initial aims or target groups, or deliberately or unintentionally delimit for whom the app is accessible or suitable. Several factors can explain shift in ambitions at the producer level. One plausible explanation suggests that targeting "the general public" may prove challenging both in terms of engagement and profitability potential – as one producer notes:

> We understood quite early on that if we were to create a commercial solution out of this endeavor, we would have to clarify our users – those who possess both a need and a willingness and ability to pay. (Producer L, security app for neighborhoods)

Initially conceived as a neighbourhood app for all residents within a specific geographical area, the company aimed at fostering active community engagement. Due to lack of resources, they later shifted focus towards more specific users whose interests and abilities aligned predictably with payment capabilities. Such user groups may include general or specific workplaces or organisations possessing varying levels of security responsibilities. Similarly, other initiatives originally aimed at activating general public engagement have undergone rebranding efforts transitioning towards either new or more narrowly defined users and needs. For example, very specific threats – often serious in nature – may necessitate handling through tailored routines and measures. However, focusing solely on such threats risks user rejection. Users might consider these apps irrelevant and/or difficult to relate to since they fail to address prominent issues within their lives. While this presents significant challenges when attempting to engage individuals from the broader general public, employers conversely bear obligations to prevent several specific risks making them more receptive towards utilising technologies effectively meeting those requirements. Municipalities – and by extension also schools – are particularly relevant contexts given recent legislative changes mandating Swedish municipalities to work actively to prevent crime (SFS 2023:196). This responsibilisation of local actors – such as schools, municipalities, and housing companies – reflects what Garland (2001) terms a strategy of adaptation where societies accept risk (such as crime) and risk avoidance as an inevitable part of everyday life. Security app companies are also an expression of such development. Unlike municipalities however, app companies are not legally obligated to prevent crime, granting them freedom and flexibility to pivot focus based on market demands. As illustrated by Producer L above, this adaptability allows them to navigate between addressing

broad societal safety concerns, specific user groups, and profitability. Security apps draw on the ideal of active and responsible citizens, yet responsibilisation of citizens might be hampered by market logics as these individuals are, at times, difficult to engage, leading to a shift from a focus on the general to the particular public, or from the public to professionals.

Although security technologies are framed as inclusive and broad in scope, not everyone has equal access to these technologies. As Costanza-Chock (2020) emphasises, technologies are rarely equally available or perceptible across all societal groups. These apps assume, as previously discussed, that insecurity is tied to specific locations that can be avoided or improved through app use. However, structural disadvantages and lived experiences of insecurity are often silenced or rendered insignificant. Furthermore, security measures such as alarm functions or the presence of security guards do not benefit everyone equally; whether security guards evoke feelings of safety or fear largely depends on one's social position. We interpret these exclusionary dimensions as a result of how certain apps disafford some of their potential users.

"Non-use", however, is a result of a reciprocal process in which abandonment occurs at both the producer level and in the everyday lives of potential users. Disaffordances and exclusionary dimensions are built into security apps, but producers also struggle to engage users. In the following section, we will explore users' actual engagement with security apps, alongside an analysis of the challenges and disaffordances associated with this engagement, all while considering the lens of producers' intended affordances.

User engagement: (dis)affordances and abandonment in everyday life

The previous section outlined the intended users and uses of these apps, essentially describing their potential feasibility. This section continues by examining user engagement from the users' perspectives, addressing how they interact with the possibilities offered by these apps. Our examples are drawn from apps targeting both the general public and workplaces, with a particular focus on child tracking apps. These apps are illustrative as they are marketed to protect a particularly vulnerable group – children – from potential dangers, while their use occurs within highly mundane contexts.

Needless to say, user engagement is key for the producers of security apps. There is an evident struggle related to user engagement, as many apps remain unused. Some apps disappear from the market entirely, while others linger in app stores without software updates, accurate information, or engagement in terms of user reviews. A "successful" app can thus be defined as one that is used. To achieve this, apps must solve problems and meet needs. Users often reproduce securitisation discourses and reaffirm the intended needs articulated in the previous section, but they also express specific needs that vary among different users. For individuals, such as parents or neighbourhood residents, apps must add tangible value to their everyday lives. For organisations like municipalities or workplaces, apps must fulfil previously unmet functions. For example, one user described how their workplace implemented a security app:

> We saw the opportunity to actually signal to each other and warn about different types of events, which schools perhaps haven't had the same opportunity to do for some time. So, we saw it as a good opportunity to increase safety for students and staff. (User H, security app for workplace and organisations)

This example illustrates how introducing a security app in the workplace is perceived as a means of taking responsibility for the safety of both staff and students. The need arises from these actors' obligations to proactively manage risks, even unlikely ones, such as ongoing lethal violence. These organisational responsibilities, along with the use of security apps to meet such responsibilities, contribute in reinforcing perceptions of risks and insecurities in mundane life. When existing systems or procedures are deemed flawed or insufficient in addressing such risks, new technologies appear to provide solutions – even if the respective risk they target are minimal. Communication capabilities enabled by these apps are often highlighted as critical. The intended use of the communication functions as articulated by the producers is thus emphasised. At the same time, users also report challenges in the new communication functions such as accidental alarms or important information being overlooked amidst overwhelming communication flows.

Abandonment, imagined scenarios, and mundane surveillance

As discussed earlier in the section on intended affordances and producer perspectives, producers frequently reframe their apps, sometimes abandoning users or objectives. Conversely, other apps have broadened their scope in terms of both functions and target audiences. For instance, apps initially designed for narrow crime prevention purposes – often targeting specific threats – have been adapted to address other risks as well. One employer at an educational workplace highlighted how the app referred to above was implemented because of employer responsibility to work proactively to handle risks that could be addressed by alarm functions. Originally developed to handle ongoing lethal violence, the function to alarm turned out to be useful for broader critical events, such as fires. The producer responded to this demand, illustrating the ongoing co-production of affordances between producer and users. It also shows how new forms of use can challenge previously potentially exclusionary objectives, such as using alarms to notify hard-of-hearing staff during emergencies.

Similar to users from organisations, users from the general public draw on, and in a sense reproduce, overarching securitisation discourses. They engage with apps both through imagined scenarios and functions, and with the functions themselves. Imagined scenarios refer to how users, through their imagination of a security threat scenario, engage in "almost use". Users of individual security apps mention things like feeling safe walking home while "almost pushing the alarm button", while users of child tracking apps mention how they think of potential risks such as terror attacks "that can happen", which motivates them using the apps:

> Interviewee: Yes, I think it's that I feel the app gives me a sense of security, being able to see where the children are if I can't reach them, if something happens. So, yes ...
> Researcher: Are there any specific problems? If something happens, are there any specific situations you have in mind?
> Interviewee: Not that I constantly worry, but yes, like my oldest son, he can go into the city sometimes on weekends. But a lot of things happen. And the terror attack on Drottninggatan or whatever it might be. I mean, you know things can happen even if the risk is small, but things can still happen, and then I think it's a bit comforting, a security to be able to see, and also just in everyday situations when they travel by public transport by themselves and so on. (User A, security app for specific publics)

The interviewee connects the use of the app to serious events like terrorist attacks, compounded by the fear of losing track of their children. The potential threats in such engagement are sometimes outspoken (fear of shootings, terrorist attacks or abductions of one's child), but as often they are merely built on vague descriptions. Imagination is required when it comes to need (security threat), function (alarm or information) as well as actual use. The fear of certain events, coupled with a responsibility to keep children safe, contribute to abstract motivations for one's use of the technology as well as to concrete engagement with the app. The interviewee then moves on to more mundane situations, like public transportation and examples of logistics and traffic, and to an uncertainty if the child will manage to navigate in public transport or find their way in new areas. Tracking the phones of children in situations where they are to travel by public transport far from home or late in the evening are activities which are motivated by an attempt to keep children safe. But in these examples, the risk does not merely translate into a dramatic external threat; risk is also linked to logistics and traffic, and to an uncertainty if the child will manage to navigate in public transport or find their way in new areas.

App use is thus motivated to handle fear of catastrophic events, offering reassurance and ease when locating children. However, many parents recognise that the sense of security provided by the tracking app, is, to some extent, illusory. Knowing a child's location does not reveal their actual activities or behaviour, and the app in itself cannot protect children from unpredictable dangerous events. While the primary motivation for using the app is ostensibly to ensure children's safety, its primary function appears to be influencing the parents' emotional state rather than directly safeguarding the child.

For many users, apps serve logistical purposes such as checking if a child has left school or ensuring dinner preparation aligns with their return home. Undramatic everyday puzzles seem to play just as prominent a role for their actual use of apps. Related to that, apps also provide another, maybe just as important, function: obtaining information about the children's location, and in that to be reassured, without having to bother them by texting or calling. This mundane use thereby often replaces direct communication:

> I think the app is convenient, but I can also realise that if I feel a little, just a little bit worried, or if I know my eldest son is in the city with some friends and I want to keep an eye on things ... I would feel much more like a nagging mom if I kept calling and texting, but now I can calm myself a bit by looking at the app without him knowing that I have ... He doesn't need to actively know that I checked tonight to see where he was, you know. So, I think that's an advantage of the app. I can use it without him knowing that I'm doing it at that moment, even though he knows I have it. (User B, security app for specific publics)

Although there are examples where children and parents communicate frequently as a result of the app – such as children requesting rides from their parents after checking their location – the main use seems to be one-way. One of the explicit goals of using the app is to avoid being perceived as a "nagging mom", which is achieved through a form of silent, "mundane surveillance" that allows parents to gather information without directly engaging with or bothering their children. This mundane use of and reliance on technology for information is also often motivated by a combination of curiosity and a desire for information about the children's whereabouts. Parents describe using the apps to gain insight into their children's everyday lives, such as during school trips, or, for separated parents, when the children are spending time with their other parent. In this context, the information retrieved through the app replaces traditional forms of obtaining information through communication. The app affords a way for parents to care for their children "at a distance", allowing them to monitor their children's activities without the need for direct dialogue.

Though many security apps are promoted as tools to enhance communication between people, in this case, they appear to render communication superfluous. The app functions as a substitute for the communication gaps experienced by some parents, allowing them to feel connected without the need for verbal exchanges. This purpose of use becomes particularly evident when parents describe how they use tracking technology to make everyday life convenient. For instance, they check the app to confirm whether their child has left school, finished training, or is at a friend's house, ensuring that everything is proceeding smoothly. Beyond mere curiosity, the interviewees also express that knowing how far their child is from home helps them plan daily activities, such as when to start preparing dinner. In these everyday scenarios, the app transcends its role as a security tool, it becomes a means to facilitate the smooth functioning of everyday life without interrupting their children with phone calls or messages.

Disaffordances and Inequalities

As we have seen, engagement with parental apps is motivated by imagined threats as well as logistic problem solving related to mundane situations. Most of the interviewees emphasise that the apps provide a sense of reassurance and tranquillity by allowing parents to know their children's whereabouts. Despite their perceived benefits for parents, security apps are not without limitations. The sense of peace and comfort these apps provide depends on whether or not the information about the child's location

and movement pattern aligns with expectations and ordinary routines. Several parents describe their children as calm and well-behaved, leading to few unexpected alerts from the app. Some interviewees question their actual need for such digital solutions since their children do not appear to be "at risk". Nevertheless, the app's effectiveness at providing reassurance depends on the predictability of the child's behaviour, suggesting that the apps' affordances are regarded as more to ease parental anxiety than to directly ensure child safety. Moreover, this requirement reveals some disaffordances and inequalities associated with the app. Parents of children with risk-taking behaviour or specific vulnerabilities may find these apps less useful or even problematic. Locating a child in such cases might not result in feelings of ease but rather heightened anxiety. Moreover, one interviewee shared information that although they experienced a concrete need and wish to use the app, it would be impossible to do so, because their child would not approve it. Furthermore, they described how the prerequisite for app usage – owning a smartphone – per se, increased the child's risk-taking behaviour in terms of online communication patterns. For this family, the app was both impractical and associated with harm more than with ease.

App use, particularly in the case of child-tracking apps, relies on an implicit requirement: engagement with the technology presupposes a collective agreement between children and parents to collaborate in the shared goal of safety. This project of keeping children safe is thus constituted as a joint interest. Several interviewees describe discussing the app with their children, who reportedly appreciate the reassurance it provides. However, this collaboration often turns out to be a chimera, where parents use the app to monitor their children without being noticed by them and without their active involvement. Some interviewees note that their teenage children are granted more freedom, such as staying out later or traveling farther from home, but this freedom is contingent on accepting surveillance. Parents argue that the apps also benefit their children by allowing them to avoid frequent calls or messages. Yet this arrangement reveals a form of conditional autonomy – surveillance is the price of independence.

Power relations inherent in these technologies, as noted by Costanza-Chock (2020), extend not only into family structures but also to society at large. The disaffordances of security apps also stem from societal inequalities, where both the availability and the perceptibility (Costanza-Chock 2020) of these technologies are unequally distributed. Financial conditions, for instance, determine whether persons can afford subscriptions to apps and the necessary smart phone(s). Related to this, is the issue of place (Wacquant 2010; Bauman 2011). The social and economic conditions structuring different physical sites – as well as app producers' approach to said differences – create unequal availabilities to some apps. In addition, imaginaries and emotions invested in and connected to different places structure both the availability and perceptibility of apps. We will exemplify this abandonment of use and users through what we understand as "aspirant users", persons who proclaim an interest in security apps and their functions, but whose use is – in one way or another – made ineligible as the geographical coverage of apps results in exclusions and unequal access to the app functions. A user review highlights this:

> Was close to buying a subscription, but unfortunately saw that the entire Järva area in Stockholm is completely marked in red on the coverage map. So, I checked other cities, and it seems to be the same in other suburban areas. Please bring this up somewhere; it is obviously a deliberate choice.
> Response from company: Great to hear that you like the service. As you mentioned, we are not available in some areas in Järva, among others. We can only operate in locations where we have good access to security guards. Unfortunately, there are places both inside and outside cities where the service cannot be used, and we are constantly working to reduce those areas. (User F review and response, security app for general public)

In the quote above, an aspiring user criticises the app for insufficient coverage, and for excluding poor suburban areas. The app company's response attributes this exclusion to a lack of infrastructure, such as security guards, in specific areas. The review above was written in 2021. Despite promises to expand coverage, the producer responds that they are "constantly working" on expanding into new geographical areas; three years later, these areas remain excluded. The areas are often socially and economically disadvantaged, so called "vulnerable areas" which overlap with neighbourhoods affected by crime or by heightened insecurity.

As a result, those who might benefit most from these technologies are excluded, highlighting a bias favouring privileged over marginalised regions. As we do not know whether the apps actually work or not, rather than advocating for broader geographical coverage, this example underscores how market-driven assumptions about user need create disaffordances that exclude potential users. Disaffordances, such as exclusion of certain geographical areas, bring abandonment of users. Aspirant users are thus not only stalled from use, they are also stalled from being a user.

Place-based imaginaries also shape the emotional affordances security apps. Parents interviewed in this study indicated that the reassurance offered by tracking apps depends on the perceived safety of the child's location. If the child frequents areas deemed hazardous, the app may fail to provide emotional comfort. Consequently, these apps reproduce and reinforce a hierarchical perception of place, embedding existing inequalities into their use.

Security apps often integrate seamlessly into daily routines, yet producers frequently struggle to sustain user engagement. Reluctance to engage with these apps arises from various factors: perceived lack of risk or danger; insufficient functionality; and ethical concerns about surveillance. There is also a lack of need for specific technological solutions addressing safety, when communications channels and neighbourhood communities already exist. In addition, apps designed to manage rare but severe risks face abandonment when such events do not occur. The use of apps enabling alarm and communication at workplaces during serious events can easily be motivated for organisations and workplaces, since employers are responsible for preventing certain risks. Given that even unusual risks are "enough" reasons to motivate the app's existence, the apps do not need to succeed in taking part in everyday routines. However, if the

use is not routinised, they risk being forgotten or deemed irrelevant, as argued by one employee: "well we do have the app, but nothing happens" (Interviewee G).

Similarly, child tracking apps are used in a mundane context to streamline family routines and to make everyday life convenient. However, users of such technologies also express that these technologies should be approached cautiously. Several parents express concerns about "over-consuming" the apps, describing their use as potentially invasive or "a bit shady". Thus, there is a reluctance to becoming "too engaged" and to use the technology too much or in an irresponsible manner. This reflects the continuous reciprocal relationship between engagement and abandonment. Producers and users collectively shape the apps' affordances and limitations. While routinised use normalises these technologies, it also raises ethical questions about their broader societal impact. Thus, disaffordances and inequalities not only affect who can access these technologies but also influence how they are used and perceived.

Concluding discussion

This article examines user engagement with security apps, focusing on the preconditions for user engagement provided by producers, and users' active responses to these preconditions. By employing the concept of (dis)affordances as co-produced through the interplay of security discourses, technology, everyday life, and its actors, our analysis reveals the reciprocal relationship between the intended affordances created by app producers, the actual user engagement or disengagement, and the (dis) affordances resulting from ongoing negotiation between intentions generated within the security market and the everyday practices and routines of users. Our study contributes a nuanced understanding of the relationships between intended and actual use, highlighting how user engagement often extends beyond the specific purposes envisioned by producers. Tensions between intentions and mundane practices are for instance illustrated by the discrepancies between the envisioned communication goals of the apps and the everyday communication practices that can bring confusion or alternative logics, motives, and consequences. For example, while the apps aim to enhance communication, increased efficiency can sometimes produce the opposite effect. This phenomenon is evident in some organisational contexts where important information is overlooked amid overwhelming communication flows, as well as in the example where parents may cease direct communication with their children, instead checking their location on the app. While Ling and Lai (2016) have explored how apps have transformed communication from dyadic to group-based interaction, our findings reveal a move away from direct communication altogether in favour of mundane surveillance.

Furthermore, communication as well as other functions of security apps are secondary to overarching securitisation discourses. However, in the context of securitisation as well as the techno-utopian versus techno-dystopian debate surrounding digital technology, our findings emphasise the significance of the everyday. Rather than categorising the impact of technology as inherently good or bad, we argue that

both utopian and dystopian approaches rely on everyday practices, feeding into them in contradictive ways. The issue of securitisation serves as a prime example. Both producers and users draw upon overarching securitisation discourses; producers use them to legitimise their apps, while users invoke them to justify their usage, thereby also indirectly validating the app's existence.

It is fully understandable and rational for companies to utilise threat discourses to market their products, especially considering the contemporary insecurity and fear of crime debate in Sweden and the broader Global North. Similarly, it is reasonable for users to engage with these discourses when discussing and legitimising their app use. A fine line exists between perceived and actual needs among users of security apps, with perceived needs frequently overshadowing requirements related to fear of crime and insecurity (at least as framed by the producers). The ideal user recognises and engages with securitisation discourses, perceiving threats sufficiently to justify app use, even in absence of necessity. Consequently, motivation for app use may align more closely with constructed fears than with tangible risks. This phenomenon underscores the complex interplay between user behaviour and prevailing security narratives, suggesting that while individual experiences may vary, overarching security discourses remain largely unchallenged.

However, it is crucial to recognise that these discourses diverge significantly from the everyday contexts in which users engage with these apps. While users may reference security narratives, their actual practices are predominantly shaped by their mundane realities. To fully comprehend app use, it is essential to acknowledge that everyday user practices often occur far away from the threats these apps purport to address. Although mundane reasons for using apps could challenge securitisation discourses, this does not appear to be the case. Future research on security apps should recognise this gap between discourse and practice. Use of these apps often reflects relatively privileged and convenient everyday lives, where users find them useful for mundane logistical issues. This observation does not conflict with securitisation discourses; rather, these discourses are either reproduced as justifications for app use or remain unspoken. We contend that this should be a point of contention, emphasising that this is not an issue of (in)security. Rather, it reflects mundane routines of everyday life, and should not be conflated with reproducing or legitimising these apps as security-enhancing technologies for the broader issues of insecurity and fear of crime articulated in campaigns and advertising.

Importantly, the "successful use" of apps, as illustrated by our finding that these apps foster calmness for certain users, often diverges from producers' intended problem-solving goals. Instead, app usage frequently intertwines with mundane routines such as family logistics or specific work-related responsibilities, distancing itself from actual or perceived threats. The micro-context of everyday use should not be interpreted in isolation, as the proliferation of these apps relies on their integration into daily routines. Paradoxically, security apps employed for mundane purposes, which are distant from securitisation discourses, simultaneously legitimise these very discourses. This necessitates a nuanced debate that acknowledges the discrepancies between the enhancement

of perceived threats or concrete crime policy matters and the often-superficial solutions provided by the market and state actors.

Furthermore, our analysis reveals that security apps embody a duality of inclusion and exclusion, manifested through disaffordances and abandonment. Disaffordances emerge as barriers that prevent certain users from engaging with the apps due to their geographical location or similar factors, leading to abandonment of certain aspiring users. Abandonment also occurs when users reject the perceived need for or functions offered by the apps, resulting in either the disappearance of certain apps or a shift in focus regarding functions or user groups. For example, apps may shift their focus from the general public to specific professional user groups. Notably, our findings indicate that those with the most pressing security needs are not necessarily the primary users of these apps, reflecting market-driven adaptions rather than need-based solutions addressing the most pressing security concerns in society. Engagement and abandonment emerge as reciprocal processes with both producers and users influencing which affordances are available. The ambivalent nature of these technologies – not necessarily a moral imperative, but also potentially morally suspicious – might hinder public engagement. However, as app use becomes routine, it also becomes normalised, often overshadowing intentions as well as practices.

Technical limitations in so called "vulnerable areas" and the reluctance of more "risk-taking" children to participate in tracking apps, highlight some of the challenges faced in these contexts. While the apps aim to provide reassurance and ease anxiety for parents, such outcomes are contingent upon users' ability to predict the implications of the information provided. Previous studies have suggested that the use of security technologies risks reinforcing people's sense of insecurity and fear, despite the goal being the opposite (Simpson 2014). Our study builds on this literature by demonstrating that while apps can offer reassurance, certain conditions must be met for these positive emotional outcomes to materialise. Notably, our findings suggest that parents with substantial reasons for concern may not necessarily experience the intended emotional benefits of the app, underscoring the complexity of the relationship between need and use.

Users who express insecurity regarding their neighbourhoods, children, or other topics often do not represent the ideal target groups for security apps. In essence, apps are convenient when there is no friction between location and actual risk. Consequently, these apps reproduce imaginaries of place, thereby reinforcing the hierarchical order of place and location (Wacquant 2010). The power relations and disaffordances inherent in these technologies, as noted by Costanza-Chock (2020), also extend to place. Previous research has indicated that security apps are more prevalent in high-income areas (Ceccato 2019). The anxiety relief – or lack thereof – offered by these applications clearly reflects the inequalities identified in other research on discrimination and insecurity (see e.g. Mulinari 2022, 2024). Abandonment encompasses various aspects of use and user engagement. For example, producers may abandon their initial target groups and respectively, users may abandon the intended use of apps. Overall, there is a lack of engagement and a lack of interest in apps with narrow crime preventive focus,

as well as a lack of interest from the producers in the (broader) public, uncovering the non-profitability of certain user groups. The concept of abandonment emphasises the co-producing aspects of "non-use", suggesting that it is not solely as a result of technology disaffording the user.

Moreover, disaffordances extend beyond the public domain into family structures. Since this study did not include interviews with children, we cannot determine how children perceive the affordances and disaffordances of security apps, or how they negotiate concepts of surveillance, safety, and freedom. While some previous studies have indicated negative consequences for tracked children (Malone 2007; Oostveen et al. 2014; Simpson 2014), there are also intriguing perspectives on children's creative interpretations of surveillance, moving beyond static notions of morality and control and arguing that children are vital actors from whom we can learn about surveillance (Kaufmann 2021).

Many producers advocate apps that address broad ambitions, such as enhancing overall security. At the same time, the use offered by these applications is often highly structured and formalised through quite narrow options and functions, focusing one-sidedly on certain aspects of crime and (in)security while obscuring others. Although, and maybe just because apps may not be at the forefront of the increasing digitalisation of crime policy, scholars examining security matters should not overlook the role of everyday security technologies in disseminating, reproducing, and legitimising overarching discourses that justify surveillance and control in the name of security. Our study contributes to the growing body of research on the preoccupation with safety and security within criminal policy (Hope & Sparks 2000; Hermansson 2018; Sahlin Lilja 2018). The apps explored here both arise from and contribute to this broader societal concern, reproducing imageries of danger in public spaces and reinforcing feelings of vulnerability and fear while promoting the ideal of responsible citizenship.

Moreover, although not the main focus of this study, the dynamics explored also highlight a lack of control over the data collected and shared by the apps, raising ethical considerations regarding public oversight of data. Previous research has shown that new technologies are often welcomed with great enthusiasm. While some apps have successfully integrated into the daily life of families (for instance), the parents we have interviewed demonstrate a nuanced and hesitant attitude towards the technology, stressing the importance of responsible and prudent use. This reflects an ambivalent relationship with the apps, which can also be linked to prior research on the expansion of control, suggesting that this phenomenon may represent an extension of control over young individuals. However, this expansion is not without its uncertainties.

In conclusion, while security apps signify a growing trend in crime prevention and security enhancement, as we have discussed, our study underscores the divergence between their intended purposes and actual use of apps. Our approach has not been devoted to whether the apps are effective or not. Instead, we aim to address the "everydaying" processes of their use, highlighting how these technologies' co-presence (Michael 2000) with users' futures (e.g. of potential threats drawn from securitisation discourses) and presents (e.g. of mundane practices in everyday life) legitimise their

use. Future research should continue to explore the mundane context of these technologies. By focusing on the everyday and its actors we can avoid simplistic dichotomies that predetermine for us what to know and think about the dissemination of such technologies, the reproduction of securitisation discourses, and their potential and actual effects on morality, surveillance, and responsibilities. Because, as this study has demonstrated, user engagement with security apps can bring many different outcomes. From easing of (perceived) anxiety to fostering abandonment, from intention to action, and from affordances to disaffordances and disengagement. These dynamics, along with the interplay between market profits and mundane routines, contribute to how our societies engage with these technologies.

Acknowledgements

We are very grateful for the insightful and helpful comments by the two anonymous reviewers and the editors. We also would like to thank Amanda Hederberg for contributing with data collection during spring 2024. Last but not least, we would like to thank all interviewees for sharing their perspectives with us.

Funding

This research was funded by Länsförsäkringar Research Foundation.

References

Aas, K. (2006) "Ta vare på deg selv, lommeboka, mobile og dine venner", 73–95 in T.H. Eriksen (Ed.) *Trygghet*. Oslo: Universitetsforlag.

Akrich, M. & B. Latour (1992) "A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies", 259–264 in W.E. Bijker & J.Law (Eds.), *Shaping Technology/ Building Society: Studies in Sociotechnical Change*. Cambridge: The MIT Press.

Andersson, R. (2010) "Tryggare kan ingen vara. En svensk kriminalpolitik för 2000-talet", 141–163 in T. Hjort, P. Lalander & R. Nilsson (Eds.) *Den ifrågasatte medborgaren. Om utsatta gruppers relation till välfärdssystemet*. Växjö: Linnéuniversitetet.

Andreassen, R., A. Kaun & K. Nikunen (2021) "Fostering the data welfare state: A Nordic perspective on datafication", *Nordicom Review* 42 (2):207–223. https://doi.org/10.2478/nor-2021-0051

Barth, S. & M.D. De Jong (2017) "The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review", *Telematics and informatics* 34 (7):1038–1058.

Bauman, Z. (2006) *Liquid fear*. Cambridge: Polity Press.

Bauman, Z. (2011) *Community. Seeking safety in an insecure world.* Cambridge: Polity Press.

Bloomfield, B.P., Y. Latham & T. Vurdubakis (2010) "Bodies, technologies and action possibilities: When is an affordance?", *Sociology* 44 (3):415–433. https://doi.org/10.1177/003803851036246

Broeker, F. (2023) "We went from the anonymity of the internet into my private WhatsApp': Rituals of transition among dating app users in Berlin", *New Media and Society* 25 (10):2551–2571. https://doi.org/10.1177/146144482110292

Bucchi, M. & B. Trench (2014) *Routledge handbook of public communication of science and technology*. Abingdon: Routledge. https://doi.org/10.4324/9781003039242

Bucher, T. (2016) "The algorithmic imaginary: exploring the ordinary affects of Facebook algorithms", *Information, Communication & Society* 20 (1):30–44. https://doi.org/10.1080/1369118X.2016.1154086

Ceccato, V. (2019) "Eyes and apps on the streets: From surveillance to sousveillance using smartphones", *Criminal Justice Review* 44 (1):25–41. https://doi.org/10.1177/0734016818818696

Chand, D., S. Nayak, K.S. Bhat, S. Parikh, Y. Singh & A.A. Kamath (2015) "A mobile application for women's safety: WoSApp". 1–5 in *TENCON 2015 - 2015 IEEE Region 10 Conference*. https://doi.org/10.1109/TENCON.2015.7373171

Charmaz, K. (2006) *Constructing grounded theory: a practical guide through qualitative analysis*. London: Sage.

Chatterjee, R., P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy & T. Ristenpart (2018) "The spyware used in intimate partner violence", 441–458 in 2018 IEEE Symposium on Security and Privacy (SP)

Costanza-Chock, S. (2020) *Design justice: Community-led practices to build the worlds we need*. London: The MIT Press. https://doi.org/10.7551/mitpress/12255.001.0001

Cumiskey, K.M. & K. Brewster (2012) "Mobile phones or pepper spray?", *Feminist Media Studies* 12 (4):590–599. https://doi.org/10.1080/14680777.2012.741893

Dieter, M., C. Gerlitz, A. Helmond, N. Tkacz, F. van der Vlist & E. Weltevrede (2018) *Store, interface, package, connection. Methods and propositions for multi-situated app studies*. CRC Media of cooperation working paper series, vol. 4. Collaborative Research Center 1187, Siegen: University of Siegen. https://www001.zimt.unisiegen.de/ojs/index.php/wps1187/article/view/29/31

Engestrom, Y. (1990) *Learning, Working and Imagining: Twelve Studies in Activity Theory*. Helsinki: Orienta-Konsultit.

Fassin, D. (2014) "Petty states of exception: The contemporary policing of the urban poor", 104–117 in M. Maguire, C. Frois & N. Zurawski (Eds.) *The anthropology of security: Perspectives from the frontline of policing, counter-terrorism and border control*. London: Pluto Press.

Fawaz, M. & H. Bou Akar (2012) "Practicing (in)security in the city", *City & Society* 24 (2):105–109. https://doi.org/10.1111/j.1548-744X.2012.01070

Ferguson, A.G. (2017) *The rise of big data policing. Surveillance, race, and the future of law enforcement*. New York: New York University Press.

Flensburg, S. & S.S. Lai (2022) "Datafied mobile markets: Measuring control over apps, data accesses, and third-party services", *Mobile Media and Communication* 10 (1):136–155. https://doi.org/10.1177/20501579211039066

Flyghed, J. & M. Hörnqvist (2003) *Laglöst land*. Stockholm: Ordfront.

Franko, K., H.O Gundhus & H.M. Lomell (2008) *Technologies of insecurity. The surveillance of everyday life*. Abingdon: Routledge-Cavendish.

Fraser, C., E. Olsen, K. Lee, C. Southworth & S. Tucker (2010) "The new age of stalking: Technological implications for stalking", *Juvenile and family court journal* 61 (4): 39–55. https://doi.org/10.1111/j.1755-6988.2010.01051.x

Garland, D. (1996) "The limits of the sovereign state. Strategies of crime control in contemporary society", *British Journal of Criminology* 36 (4):445–471. https://doi.org/10.1093/oxfordjournals.bjc.a014105

Garland, D. (2001) *The culture of control*. Oxford: Oxford University Press.

Gibson, J.J. (1966) *The senses considered as perceptual systems*. London: Houghton Mifflin.

Gibson, J.J. (1979) *The ecological approach to visual perception*. London: Houghton Mifflin.

Hermansson, K. (2018) "Den svenska tryggheten: en studie av en kriminalpolitisk symbol", *Sociologisk Forskning* 55 (2–3):179–202. https://doi.org/10.37062/sf.55.18189

Hermansson, K. (2023) "Emotional expressions in the Swedish discourse on crime. A comparison of the 2018 Moderate and Social Democratic election campaigns", *Sociologisk forskning* 60 (1): 33–55. https://doi.org/10.37062/sf.60.24779

Hope, T. & R. Sparks (2000) *Crime, risk and insecurity*. London: Routledge. https://doi.org/10.4324/9780203389492

Hutchby, I. (2001). "Technologies, texts and affordances", *Sociology* 35 (2):441–456. https://doi.org/10.1177/S0038038501000219

Hutchby, I. (2003). "Affordances and the analysis of technologically mediated interaction: A response to Brian Rappert", *Sociology* 37 (3):581–589. https://doi.org/10.1177/00380385030373011

Interaction Design Foundation (2024), "Affordances," retrieved April 12 2025,
from https://www.interaction-design.org/literature/topics/affordances.

Kaufmann, M. (2021). "This Is a Secret: Learning from children's engagement with surveillance and secrecy", *Cultural Studies – Critical Methodologies* 21 (5): 424-437. https://doi.org/10.1177/15327086211029350

Kennedy, L. & M. Coelho (2022) "Security, suspicion, and surveillance? There's an app for that", *Surveillance and Society* 20 (2):127–141. https://orcid.org/0000-0003-3012-5544

Kettrey, H. H., M.L. Tidwell, S.R. Burke, S. Duncan, M. Nwajei, N.S. Reynolds, C. Waddell, S. Scott, C. Imbody, M. Jerge, J. Young, N. Nishan, A. Rathi & J. Jackson (2024) "Crime control or just theater? An experimental test of the effects of a mobile safety app on crime prevention intentions and behaviors", *Journal of Experimental Criminology*, Advance online publication. https://doi.org/10.1007/s11292-024-09613-0

Lai, S. & S. Flensburg (2020a) "A proxy for privacy uncovering the surveillance ecology of mobile apps", *Big Data and Society* 7 (2):1–20. https://doi.org/10.1177/2053951720942543

Lai, S.S. & S. Flensburg (2020b) "Appscapes in everyday life: Studying mobile datafication from an infrastructural user perspective", *MedieKultur: Journal of Media and Communication Research* 36 (69):29–51. https://doi.org/10.7146/mediekultur.v36i69.121018

Ling, R. & C.H. Lai (2016) "Microcoordination 2.0: Social coordination in the age of smartphones and messaging apps", *Journal of Communication* 66 (5):834–856. https://doi.org/10.1111/jcom.12251

Low, S. (2008) "Fortification of residential neighbourhoods and the new emotions of home", *Housing, Theory and Society* 25 (1):47–65. https://doi.org/10.1080/14036090601151038

Lupton, D. (2012) "M-health and health promotion: The digital cyborg and surveillance society", *Social Theory and Health* 12 (10):229–244. https://doi.org/10.1057/sth.2012.6

Lupton, D. (2014) "Critical perspectives on digital health technologies", *Sociology Compass* 8 (12):1344–1359. https://doi.org/10.1111/soc4.12226

Maxwell, L., A. Sanders, J. Skues & L. Wise (2020) "A content analysis of personal safety apps: are they keeping us safe or making us more vulnerable?" *Violence against women* 26 (2):233–248. https://doi.org/10.1177/1077801219832124

McVeigh-Schultz, J. & N.K. Baym (2015) "Thinking of you: Vernacular affordance in the context of the microsocial relationship app, couple", *Social Media + Society* 1(2). https://doi.org/10.1177/2056305115604649

Maguire, M., C. Frois & N. Zurawski (2014) *The anthropology of security: Perspectives from the frontline of policing, counter-terrorism and border control*. London: Pluto Press.

Malone, K. (2007) "The bubble-wrap generation: children growing up in walled gardens", *Environmental Education Research* 13 (4):513–527. https://doi.org/10.1080/13504620701581612

Masco, J. (2014) *The theatre of operations: National security affect from the Cold War to the war on terror*. Durham: Duke University Press.

Massumi, B. (2005) "Fear (the spectrum said)", *Positions: East Asia Cultures Critique* 13 (1):31–48. https://doi.org/10.1215/10679847-13-1-31

Messing, J., M. Bagwell-Gray, M.,M.L. Brown, M. L., A. Kappas, A., & A. Durfee, A. (2020). "Intersections of stalking and technology-based abuse: Emerging definitions, conceptualization, and measurement"., Journal of Ffamily Vviolence, 35 (7):, 693–-704. https://doi.org/10.1007/s10896-019-00114-7

Michael, M. (2000). These Boots Are Made for Walking...: Mundane Technology, the Body and Human-Environment Relations. Body & Society, 6(3-4), 107-126. https://doi.org/10.1177/1357034X00006003006 (Original work published 2000)

Michael, M. & D. Lupton (2016) "Toward a manifesto for the 'public understanding of big data'", *Public Understanding of Science* 25 (1):104–116. https://doi.org/10.1177/0963662515609005

Morris, J.W. & E. Elkins (2015) "There's a history for that: Apps and mundane software as commodity", *Fibreculture Journal* (25):62–87. https://doi.org/10.15307/fcj.25.181.2015

Mulinari, L.S. (2022). *Folkets Husbys trygghetsundersökning 2022: Communityperspektiv på kriminalitet och utsatthet.* Stockholm: Folkets Husby.

Mulinari, L.S. (2024). *Folkets husbys trygghetsundersökning 2024: Tidöavtalet och omförhandlingen av samhällskontraktet.* Stockholm: Folkets Husby.

Neocleous, M. (2008) *Critique of security*. Edinburgh: Edinburgh University Press. https://doi.org/10.1515/9780748632329

Norman, D.A. (1988) *The design of everyday things*. New York: Basic Books.

Oostveen, A., M., A. Vasalou, A., P. Van den Besselaar , P., and I.& Brown , I. (2014). "Child location tracking in the US and the UK: Same technology, different social implications",. Surveillance & Society, 12 (4):, 581–-593. https://doi.org/10.24908/ss.v12i4.4937

Pink, S., S. Sumartojo, D. Lupton & C. Heyes La Bond (2017) "Mundane data: The routines, contingencies and accomplishments of digital living", *Big Data and Society* 4 (1). https://doi.org/10.1177/2053951717700924

Rappert, B. (2003) "Technologies, texts and possibilities: A reply to Hutchby", *Sociology* 37 (3): 565–580. https://doi.org/10.1177/00380385030373010

Riddell, A. (2023) "Intersecting positionalities and the unexpected uses of digital crime and safety tracking in Brooklyn", *Social Inclusion* 11 (3):30–40. https://doi.org/10.17645/si.v11i3.6615

Sahlin Lilja, H. (2018) "'Otrygghet' i politisk kommunikation: En begreppslig jämförelse och analys av 1970 and 2010-talen", *Nordisk tidsskrift for kriminalvidenskab* 105 (2):170–190. https://doi.org/10.7146/ntfk.v105i2.120551

SFS 2023:196. *Kommuners ansvar för brottsförebyggande arbete*. (Swedish statute).

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

Stanko, E. (2000) "Victims r us. The life history of 'fear of crime' and the politicization of violence", 13–30 in T. Hope and R. Sparks (Eds.) *Crime, risk and insecurity*. London: Routledge. https://doi.org/10.4324/9780203389492

Viswanath, K. and A. Basu (2015) "SafetiPin: an innovative mobile app to collect data on women's safety in Indian cities", *Gender and Development* 23 (1):45–60. https://doi.org/10.1080/13552074.2015.1013669

Wacquant, L. (2010) *Urban outcasts: A comparative sociology of advanced marginality*. Cambridge: Polity Press.

White, D. and L. McMillan (2020) "Innovating the problem away? A critical study of Anti-rape technologies", *Violence against women* 26 (10):1120–1140. https://doi.org/10.1177/1077801219856115

Winter, K. (2025) "Longing and lacking: Pasts, presents, and futures in municipal crime prevention technology", *Nordic Journal of Science and Technology Studies,* 13 (1). https://doi.org/10.5324/njsts.v13i1.5857

Wood, M.A., S. Ross & D. Johns (2022) "Primary crime prevention apps: A typology and scoping review", *Trauma, Violence and Abuse* 23 (4):1093–1110. https://doi.org/10.1177/1524838020985560

Woolgar, S. (2002)"After word? – On some dynamics of duality interrogation", *Theory, Culture & Society* 19 (5-6):261–270. https://doi.org/10.1177/02632760276189925

Young, A. (1996) *Imagining crime. Textual outlaws and criminal conversations*. London: Sage.

Zuboff, S. (2019) *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London: Profile Books.

Author presentations

Katarina Winter is Doctor in Sociology and Senior Lecturer in Criminology at the Department of Criminology, Stockholm University.
Contact: katarina.winter@criminology.su.se

Klara Hermansson is Doctor and Senior Lecturer in Criminology at the Department of Social Work, Criminology and Public Health Sciences, University of Gävle.
Contact: klara.hermansson@hig.se