POLSKA AKADEMIA NAUK • INSTYTUT NAUK PRAWNYCH

ZAKŁAD KRYMINOLOGII

ARCHIWUM KRYMINOLOGII

Archives of Criminology

PL ISSN 0066-6890

DOI 10.7420/AK2024.13

2024 • 46(1) • 149–179

Veronika Nagy ■

Social sorting in Europe: Self-censorship in a digital asylum

Sortowanie społeczne w Europie. Autocenzura w cyfrowym azylu

Abstract: In recent decades, global mobility control and digital surveillance measures have increasingly prioritised affective aspects and perception-based policies. However, these practices encounter resistance, particularly in the everyday use of connected migrants. Through qualitative data analysis within the tradition of critical surveillance studies, this paper investigates how marginalised mobile groups – often labelled suspects of terrorism and organised crime – circumvent mobile surveillance and social sorting mechanisms within and beyond Fortress Europe. Rising tech literacy and surveillance awareness among users challenge digital policing, reshaping interactions between suspected newcomers and border control authorities. While existing studies focus on countersurveillance activities, less attention is given to strategic "silences" and social filters used to evade profiling and sorting mechanisms, protecting those who fear the risks of crossing a border. Based on notions of secure connectivity, this research employs a multi-site analysis of refugee polymedia use to examine countersurveillance strategies and digital self-censorship practices in transit countries.

Keywords: surveillance, censorship, hardware, imaginaries, migration

Abstrakt: W ostatnich dziesięcioleciach w ramach globalnej kontroli mobilności i nadzoru cyfrowego coraz częściej priorytetowo traktowane są aspekty afektywne i polityka oparta na percepcji. Praktyki te napotykają jednak na opór, zwłaszcza w codziennym korzystaniu z sieci przez migrantów. Przy użyciu jakościowej analizy danych w ramach tradycji krytycznych badań nad inwigilacją, niniejszy artykuł ma na celu zbadanie, w jaki sposób zmarginalizowane grupy mobilne – często określane jako podejrzane o terroryzm i przestępczość zorganizowaną – obchodzą mechanizmy mobilnej inwigilacji i sortowania społecznego w obrębie Twierdzy Europa i poza nią. Rosnąca wiedza technologiczna i świadomość nadzoru wśród użytkowników sieci stanowią wyzwanie dla policji cyfrowej i przekształcają interakcje między podejrzanymi przybyszami a organami kontroli granicznej. Podczas gdy istniejące badania koncentrują się na aktywnościach przeciwdziałających inwigilacji, mniej uwagi poświęca się strategicznemu „milczeniu" i filtrom

Dr Veronika Nagy, Utrecht University, the Netherlands, v.nagy@uu.nl, ORCID: 0000-0002-4522-8493

społecznym wykorzystywanym do unikania mechanizmów profilowania i sortowania, chroniącym tych, którzy obawiają się ryzyka związanego z przekraczaniem granicy. W nawiązaniu do koncepcji bezpiecznego połączenia w artykule wykorzystano wielostanowiskową analizę korzystania przez uchodźców z polimediów, aby zbadać strategie przeciwdziałania inwigilacji i praktyki autocenzury cyfrowej w krajach tranzytowych.

Słowa kluczowe: inwigilacja, cenzura, sprzęt komputerowy, zbiorowe wyobrażenia, migracja

Introduction

"This is all left from me", he said, showing his SIM card attached to his necklace with some scratched numbers on it. The volunteer of the German language school in one of the Asylum Application centres was sitting with me, sipping tea, venting about his lost life and the endless limbo of his administrative uncertainties in a small German city. It catches my eyes when he holds this little chip between his fingers as an amulet.[1] A worthless little chip in a frame turned into a symbol of a lost life as a passport for self-identification.

The intersection of political conflicts and new border surveillance practices has significantly transformed the experiences of refugees along key migration routes, particularly the Balkan route. Syrian and Afghan refugees – fleeing conflict and seeking safety in Europe – now face not only physical borders, but also sophisticated digital surveillance systems designed to monitor and control their movements (Bigo 2008; Lyon 2010). These surveillance mechanisms, deeply embedded in the migration infrastructure, such as biometric authentication tools (Leese 2022), force refugees to adopt strategies of self-censorship that go beyond merely controlling the content of their communications online. Instead, with rising surveillance awareness, resistance strategies extend to managing the very materialities of their digital connectedness: the devices they use, the networks they connect to and the ways they interact with mobile hardware technologies unwillingly alter the credibility of connected devices as identification tools in migration control processes, such as asylum applications (Latonero, Kift 2018).

Therefore, this paper examines the materialities of surveillance awareness and self-censorship practices of Syrian and Afghan refugees along the Balkan route, with a focus on hardware selection and retrospective narratives on mobile phone security and data protection on the move. Unlike traditional notions of self-censorship, which often focus on suppressing linguistic or written content, this study explores how refugees manage the material aspects of their digital connectivity to

[1] A SIM card, or Subscriber Identity Module, is a small chip that can be inserted into a mobile device to activate it and connect it to a network. This card, as a global communication tool, contains unique information that identifies the user to the network and enables the device to receive and transmit calls, texts and data. The SIM card also stores contact information, messages and other data associated with the user's account as a dynamic archive beholding the traces of unpredicted journeys and traumas.

avoid detection (Nalbandian 2022). The central research question asks: How do refugees engage with the social imaginaries of mobile hardware technologies in shaping self-censorship practices within the context of border control surveillance?

In recent years, smartphones have become essential tools for refugees, offering crucial connectivity for navigation, communication and accessing resources (Dekker et al. 2018; Nedelcu, Soysüren 2022). However, these devices also serve as a critical point of vulnerability (Rayes, Salam 2022). Refugees are acutely aware that the materialities of their digital lives – such as the specific phone they use, the SIM card they purchase or the apps they install – can expose them to surveillance by state actors or border authorities (Gonzalez, Deckard 2022; Pallister-Wilkins 2022). This awareness shapes their self-censorship practices, not just by limiting what they say, but by determining how, when and through which devices they connect to mobile networks.

The concept of self-censorship among refugees in the context of mobile phone use is embedded in a broader, complex matrix of surveillance, state control and refugee agency (Filak 2010). This practice emerges as a response to the perceived threats associated with the technological landscape that refugees must navigate. Self-censorship, in this sense, represents a range of strategies that aim to mitigate the risks of surveillance, monitoring and potential exposure to hostile state mechanisms or third parties (Tanczer et al. 2020). These strategies encompass a diverse array of practices, from selective communication to repurposing technological tools in a manner akin to "hacking" systems of control, offering both protection and agency to refugees (Wang, Ahmed, Bee 2024). Drawing from critical surveillance studies, digital migration and border criminology, this paper reveals how refugees conceptualise the security of their mobile hardware and data, engaging in practices of self-censorship that are embedded in the situationally changing material realities of their digital existence (Učakar 2020; Minca, Collins 2021). Refugees along the Balkan route developed specific imaginaries of mobile hardware, associating particular devices or digital tools with safety, privacy or increased risk. The materialities of digital connectedness – which include choices about hardware, operating systems, encryption features and curated network access – provide a symbolic representation of the changing technological myths and beliefs that explain how refugees adjust their self-censorship practices.

It was noted in the early waves of the 2015 migration crisis that some refugees prefer iPhones over Android devices due to their perceived stronger encryption, while others use "burner phones" – temporary or disposable phones that are discarded after a short period of use – or physically disconnect from all connectable devices to minimise traceability (Campesi 2021; Ozkul 2023). These practices raised concerns about the strategic engagement of refugees with mobile technologies (Hesselberth 2018), associating them with organised crime tactics such as identifiers of trafficker networks, where the avoidance of detection is not just about limiting verbal or textual content, but about navigating the physical and technological infrastructures of connectivity. This engagement is a form of

self-censorship that operates at the level of hardware and device management, illustrating the complex ways in which refugees negotiate their digital presence in the context of surveillance (Lyon 2010; Gonzalez, Deckard 2022). Following the definition of Bar-Tal, self-censorship is defined as the act of intentionally and voluntarily suppressing information from others when formal impediments are absent. Self-censorship hinders the proper functioning of a democratic society because it inhibits free access to information, freedom of expression and the flow of information. The role of self-censorship in societies is of vital importance, as it blocks information that may illuminate various societal issues. Nevertheless, it is assumed that in some cases self-censorship is necessary (Bar-Tal 2017).

Current studies in digital anthropology and surveillance studies provide a critical lens for understanding how these material practices intersect with state-led efforts to control migration and surveillance (Milivojevic 2021; Deleuze 1992), but they predominantly focus on the power relations between authorities and mobile users, missing the sociotechnical cultural notions of tech imaginaries associated with the device itself. In order to prevent the risks of being identified while navigating border crossings, refugees must carefully manage their hardware selection: limiting the use of location-based services, disabling certain features and functions (such as microphones) or even disconnecting from telco networks altogether when crossing borders (Pfeifer 2021). These behaviours highlight a material form of self-censorship, where decisions about digital connectedness are just as critical as the content shared or withheld in online communication. Therefore, this research aims to explain the material dimensions of digital self-censorship in the context of forced migration along the Balkan route. This paper argues that refugees' interactions with mobile technologies are deeply influenced by the situational perceptions on surveillance risks and the socioeconomic threat associated with mobile connectivity. Rather than focussing on linguistic self-censorship and the fear of border authorities' semantic surveillance, this study emphasises how refugees' decisions about which hardware to use, when to connect and how to manage their digital footprint represent critical survival strategies. These material practices of self-censorship not only reveal the refugees' agency in resisting surveillance, but also reflect the complex entanglements between migration, technology and power in contemporary border control regimes (Petit 2020; Ozkul 2023).

By examining the imaginaries of mobile hardware technologies, this paper highlights how refugees use the Internet of Things, including mobile phone devices, to strategically manage their exposure to surveillance systems. This focus on the materialities of digital connectedness provides a new dimension to discussions of self-censorship and demonstrates how refugees leverage mobile hardware to maintain control over their digital lives while navigating the precarious conditions of border control and expulsion practices.

Methodology

This study forms part of the Digital Asylum project under the Gerda Henkel Foundation's Security and Society project stream, which investigates the surveillance awareness and behaviour modification of refugees in their mobile phone use. Conducted between 2018 and 2021, the research spans Hungary, Greece, Turkey, Germany and the Netherlands, retrospectively exploring how refugees navigated surveillance along the Balkan route. This methodology combines multi-sited ethnography, interviews, participant observation and virtual ethnography to understand how refugees adapted their mobile phone use and digital practices to evade surveillance.

The fieldwork began in Hungary, focussing on local NGOs and authorities, followed by visits to Lesvos and Athens in Greece, Izmir and Istanbul in Turkey and asylum centres in Germany and the Netherlands. Due to the COVID-19 lockdowns, some phases were conducted virtually, leveraging virtual ethnography to complement in-person fieldwork. The use of multi-sited ethnography (Falzon 2012) was crucial for capturing refugee experiences across multiple contexts, both physical and digital. This approach acknowledges the fluidity of refugee movements and the complex interaction between individuals and surveillance systems across various borders (Marcus 1995; Wahlberg 2022). The method is particularly well-suited to the study's focus on transnational mobility and refugees' behavioural adaptations in different border regimes (Hage 2005).

In total, 28 semi-structured interviews were conducted with a diverse range of professionals involved in border control and migration surveillance. These included migration authorities, border police, security intelligence officers, NGO representatives, local human rights activists and migrants from the selected sending countries. Additionally, interviews were held with experts from science and technology studies and surveillance studies to provide critical insights into the mechanisms of surveillance and the implications for migrant populations. The semi-structured format allowed for in-depth discussions while maintaining the flexibility to explore emerging themes related to surveillance practices, policy responses and the lived experiences of migrants. This methodological choice facilitated a nuanced understanding of the dynamics at play between state authorities and migrant communities and offered valuable context to the refugee experiences examined in this research. Though such interview data may be subject to biases based on my phrasing or the participants' willingness to disclose sensitive information – particularly when discussing surveillance practices (Hennink Kaiser, Weber 2019) – the diverse professional backgrounds of the interviewees, even those with conflicting perspectives, allowed an exploration of the different perceptions on refugees' surveillance awareness and behaviour modification. Some interviews were conducted in Turkey and Greece with interpreters, which also enabled the collection of retrospective accounts of how the refugees modified their behaviour

when using mobile phones in different countries and how they educated each other on the potential risks of being intercepted by local authorities. Following the Association of Social Anthropologists (ASA) guidelines, no written consent forms were used, but verbal consent was obtained in all cases. Ethical concerns, including anonymity and confidentiality, were prioritised to protect vulnerable populations, undocumented people or those assisting others in border crossings.

Participant observation as a form of institutional ethnography was conducted at two INGOs and three grassroots organisations in short periods (due to COVID-19 measures) providing essential services such as healthcare and language training. This method allowed for the observation of how NGO workers and refugees responded to perceived surveillance activities in real time. Observing these everyday interactions revealed how professionals contribute to refugees' self-censorship practices, particularly concerning their influence on mobile phone use (Scheel, Ustek-Spilda 2019), including switching SIM cards or not using certain wearables (Ozkul 2023; Pfeifer 2021). Participant observation was oftentimes emotionally demanding, as it is based on a complete immersion in the sensitive contexts of vulnerable groups, where full access to all aspects of refugee life may be limited due to security or ethical concerns. Therefore, this method has been complemented with virtual ethnography. This methodology also addressed the limitations of physical fieldwork during the pandemic and relied on OSINT data gathered from open and semi-open social media platforms, including Facebook and Telegram, where refugees and migrants exchange information on migration routes and border conditions. Online groups were identified by referencing refugee nationalities or migration terms, such as "Syrians in Izmir", and closed groups related to Moria or The Game (Dekker et al. 2018).

The combination of in-person and virtual methods allows for a more comprehensive understanding of how refugees navigate the complex surveillance systems they encounter during migration (Leurs, Smets 2018; Pfeifer 2021). Virtual ethnography, in particular, was invaluable in capturing real-time digital behaviours, which often reveal more about self-censorship than traditional interviews or participant observation (Gillespie, Osseiran, Cheesman 2018). This was a highly valuable method in understanding how mobile technologies shape refugee experiences (Gillespie, Osseiran, Cheesman 2018; Nedelcu, Soysüren 2022) and provided insights in the data that were structurally withheld by the platform users. However, verifying the identity of online participants remained a challenge, which also complicated the reliability of the data selected – as with language barriers – limiting the understanding of subtle nuances in chat conversations (Leurs, Smets 2018).

The selected methods, while comprehensive, have certain limitations. Multi-sited ethnography is resource-intensive, and not all sites could be revisited due to the COVID-19 pandemic. Interviews can be affected by recall bias, as participants may misremember or downplay certain behaviours in retrospect. Participant observation, while offering rich, in-situ data, may not fully capture the depth of self-censorship that occurs internally or digitally. Finally, virtual ethnography can

encounter issues of identity verification and language barriers, which may affect the reliability and depth of online interactions (Nagy 2024).

Considering the vulnerability of the research population, several issues were taken into consideration regarding their migration status and role in informal economies. No covert observation was conducted, and anonymity, confidentiality and digital data security were maintained, particularly for participants with vulnerable legal status. The sensitive nature of surveillance research required additional precautions to ensure the protection of refugees and NGO workers (Kerezsi, Nagy 2020). The research focusses on how refugees from Syria and Afghanistan retrospectively reflected on their surveillance awareness and behaviour modification regarding their mobile phone use.

Theoretical framework

This paper employs the concept of techno-authoritarian imaginaries to analyse the surveillance awareness and self-censorship practices of refugees from Syria and Afghanistan as they navigate the complexities of migration along the Balkan route. As identified by Hendrik Schopmans and İrem Ebetürk (2023), while the proliferation of artificial intelligence and surveillance technologies has been linked to the rise of digital authoritarianism, the resistance to such mechanisms remains an underexplored area within both migration studies and surveillance studies. Techno-authoritarian imaginaries refer to the collective perceptions and narratives that frame how societies understand and engage with technologies that exert control and surveillance (Cupać, Schopmans, Tuncer-Ebetürk 2024). These imaginaries are shaped by historical and political experiences, influencing how communities conceptualise the implications of surveillance technologies in their lives (Schopmans, Ebetürk 2023).

In the context of this study, refugees bring their own pre-existing imaginaries about authority, technology and resistance, informed by their experiences of conflict and migration. As a response to these perceptions, anticipatory resistance will be explored in the materiality of tech use (Kazansky 2021). This framework positions refugees not merely as passive subjects of surveillance, but as active agents engaging in anticipatory resistance. This form of resistance is characterised by pre-emptive actions taken by refugees to evade detection and control by surveillance systems. Rather than reacting solely to oppressive measures after they are implemented, refugees proactively modify their behaviour and mobile phone use, anticipating the risks associated with state surveillance and data exploitation. This anticipatory stance aligns with the notion that resistance can be an ongoing process, shaped by the recognition of systemic inequalities and the potential for future challenges (Schopmans, Ebetürk 2023). Therefore, the concept of "dataveillance imaginaries" is adopted as presented by Kiran Kappeler, Noemi Festic and Michael Latzer (2023), which highlights how individuals' perceptions of constant surveillance can lead to self-inhibition in their online behaviour. Similar to internet users who modify their digital communication to avoid the chilling effects of dataveillance, refugees engage in self-censorship to navigate their interactions

in a digitally surveilled environment. Awareness of surveillance leads to self-inhibition, wherein refugees refrain from using certain mobile applications, avoid sharing sensitive information or alter their communication practices altogether.

Central to the examination of refugees' surveillance awareness is the imaginary surrounding mobile phone hardware as a securitised device. Research indicates that refugees often perceive their mobile phones not only as tools for communication, but also as instruments of surveillance and control (Zhang 2023). The imaginaries tied to specific electronic device brands and models, particularly those associated with enhanced security features (e.g. encryption), inform their choices and behaviours in the context of migration. For instance, a smartphone perceived as secure may foster a sense of safety and agency, leading refugees to use it more freely. Conversely, a device associated with surveillance vulnerabilities may result in cautious behaviour, where refugees self-censor their communications or avoid using certain applications altogether. This dual perception underscores the significance of mobile phones as not only functional devices, but also as symbols of power dynamics and security in the context of migration.

Regarding such contextual variability, I will explain how the imaginaries of refugees are contingent on their unique sociopolitical backgrounds and migration experiences, leading to variations in how they engage with technology and surveillance (Schopmans, Ebetürk 2023). Syrian and Afghan refugees hold different perceptions of surveillance based on their respective experiences with authoritarian regimes and conflict. These differences influence their self-censorship strategies and how they navigate their digital connectedness while in transit. This study posits that these techno-authoritarian and dataveillance imaginaries not only shape refugees' awareness and responses to surveillance, but also serve as a basis for mobilisation against oppressive technologies, such as satellite tracking of connected devices. As refugees articulate their experiences with mobile hardware and the risks associated with surveillance, they create narratives that foster solidarity and collective resistance against the impositions of state power and policing incentives. These narratives are also crucial for advocacy efforts within civil society, drawing attention to the ethical implications of surveillance technologies and leading authorities as well as humanitarian networks to call for accountability in their use. Therefore, this critical approach enriches existing debates on resistance to autocratisation, especially in ID verification processes, and highlights the need for deeper engagement with the materialities of future-making in the context of digital migration. As refugees navigate surveillance infrastructures by hardware management, they contribute to the ongoing discourse around the social and political dimensions of digital technologies in vulnerable settings. Their lived experiences of surveillance awareness not only reveal the limitations of existing frameworks, but also advocate for a more nuanced understanding of how marginalised populations adapt to and resist techno-authoritarianism.

The incorporation of techno-authoritarian, dataveillance and mobile hardware imaginaries allows this study to explore how refugees perceive the relationship

between technology and power (Haile 2021), illustrating the importance of their digital strategies and the broader societal implications of their actions. By recognising the role of these imaginaries, this research underscores the need for critical engagement with the materialities of mobile phone use (Pink, Ardèvol, Lanzeni 2020) and the ways in which refugees enact self-censorship in response to an increasingly surveilled environment.

In the discourse surrounding border control and migration, there is a critical oversight regarding the digital materialities that underpin the experiences of refugees and migrants. While much attention has been directed toward the tech solutionism that frames surveillance technologies as straightforward answers to complex migration challenges, there is a pressing need for empirical research that examines the material aspects of these technologies (Fenwick 2015): specifically, the hardware that refugees rely on during their journeys. Understanding how mobile devices function as tools for navigation, communication and self-tracking is essential to uncovering how they shape the imaginaries of safety in the context of digitised migrant economies. These devices do not merely serve as conduits for information; they actively influence refugees' perceptions of security, agency and connectivity as they navigate precarious border landscapes (Morgan 2023).

Moreover, as security technologies transition from reactive to proactive deployment, they become not just concrete objects, but fluid expressions of power that can lead to unintended consequences (Trauttmansdorff 2022). This evolution, characterised by the invisible and automated nature of surveillance algorithms, highlights the need for critical examination of how these technologies shape social and political realities (Zureik 2010). By focussing on the material dimensions of technology, this research aims to illuminate the complex interplay between hardware, surveillance and the construction of safe spaces in the lives of migrants, challenging the dominant narratives that often neglect the lived realities of those impacted by these systems. In this context, the concept of sociotechnical imaginaries becomes crucial, as it refers to the collectively held visions of desirable futures, reflecting how societies imagine and shape their relationship with technology (Milivojevic, Biles 2017; Sánchez-Querubín, Rogers 2018; Gerhold, Brandes 2021; Nedelcu, Soysüren 2022; Trauttmansdorff 2022; Kappeler, Festic, Latzer 2023).

Imaginaries and fears of portable devices: Refugee perceptions of surveillance power in hardware vs software

Refugees, navigating the complexities of social and special trajectories, often develop nuanced perceptions of the surveillance power embedded within the technologies they use. These perceptions are shaped by their lived experiences with authorities and the sociopolitical contexts of their journeys, influencing their attitudes, especially distrust towards both hardware (physical devices) and

software (applications and platforms). The concept of surveillance imaginaries – the collective understanding and anticipation of how technologies might be used to control, track or oppress them – plays a central role in shaping their behaviour. This section explores the empirical and conceptual distinctions refugees make between hardware and software, revealing a spectrum of self-censorship practices and modes of dysconnectivity.

> When I crossed the Syrian–Turkish border, I held my phone tightly in my hand. It felt like a lifeline, but also a threat. I knew the border guards could track my location, see who I've spoken to, even read my messages. Every time I turned it on, I felt like I was exposing myself to being watched. It wasn't just a phone anymore – it was like holding a mirror to my own fear of being monitored.

For many refugees, hardware such as smartphones, laptops and SIM cards are seen as the most visible agents of surveillance. The physical nature of these devices makes them identifiable tools that can facilitate both connection and control (e.g. IP, SIM, GNSS, UMTS or EODT). As soon as a refugee holds a smartphone, it is no longer just a communication device – it becomes a potential surveillance apparatus. This visibility leads to heightened awareness and subsequent self-censorship practices aimed at mitigating the risks of being tracked.

> Before crossing, I took out my SIM card and threw it away. I didn't want anything connected to Syria in my phone – no old contacts, no data. I was afraid they'd trace me through it, or worse, think I was linked to something dangerous. From that moment, I started being careful with every SIM card I used. I wouldn't store numbers or even keep the same card for long. It wasn't just about staying safe – it was about staying invisible.

Many refugees create anonymous or pseudonymous social media accounts to shield their identities while still engaging in essential online communities (Nedelcu, Soysüren 2022). These anonymous accounts allow refugees to access information, connect with support networks and engage with diaspora communities without exposing their real identities, which could be traced back to their physical locations or immigration status. Moreover, some refugees limit or entirely avoid the use of digital platforms or hide their E-CellID, particularly those that require personal information or regular updates. This restricted access, or even full disengagement from digital tools, is often seen as a strategy to reduce the digital footprint that could be exploited by surveillance actors (Sadowski 2020).

Similarly, the GPS and GMS tracking capabilities embedded in most smartphones are a primary source of fear among many refugees, as it directly translates to the possibility of real-time surveillance of their movements. Research by Shahram Khosravi (2017b) highlights how refugees develop an acute awareness of how mobile hardware can be used to monitor them, leading to behavioural adaptations such as turning off location services, removing SIM cards or even switching to simpler, non-smartphone devices that offer less tracking capability.

> Every step I took felt like walking a tightrope between the migration authorities and the regime back home. I knew that if either side caught wind of my movements, I could disappear. I turned off my GPS and erased my location history, fearing that even a moment of carelessness could expose me to both sets of authorities. Sharing my whereabouts became a luxury I couldn't afford, even with those I trusted.

The tangible nature of the hardware, which can also be confiscated, compounds these fears. A refugee's mobile device is a physical object that can be taken by authorities during checkpoints or border crossings. Nicholas De Genova (2013) emphasises that the confiscation of mobile phones often exposes refugees' private information – such as contacts and sensitive communications – to authorities, creating a pervasive sense of paranoia about their hardware use. In response, many refugees deliberately avoid storing critical information on their primary devices, preferring instead to use burner phones or to employ encrypted storage systems, reflecting a tactical awareness of the risk of device seizure. As one young Syrian man explained in Istanbul:

> I learnt to rely on burner phones, which I bought from street vendors in crowded markets. It felt risky, but I knew I had to protect myself from both migration authorities and the regime back home. Each time I got a new phone, I felt a mix of relief and anxiety. I couldn't save any contacts or store messages; everything had to be temporary and disposable. I kept my conversations brief and avoided anything that could trace back to me.

Managing devices to evade surveillance is an underestimated component of self-censorship. Refugees often rely on burner phones to maintain anonymity and minimise the risk of long-term tracking (Sadowski 2020). This practice aligns with the notion of "deportability", a term coined by Nicholas De Genova (2002), which highlights the constant threat of expulsion and the precarious legal status that forces migrants to engage in practices that reduce their visibility to state systems. The type of hardware selected also reflects the imaginaries of security. Refugees increasingly prefer devices perceived to be more secure, such as those with advanced encryption or non-mainstream brands. Guoliang Zhang (2023) found that many refugees opted for smartphones like certain Android models known for stronger encryption standards over more popular brands like iPhones, which they associated with higher risks of surveillance. These choices reflect a techno-authoritarian imaginary (Aouragh, Chakravartty 2016), where refugees believe specific brands or hardware configurations are more resistant to government control, shaping their hardware preferences and behaviours. As a community worker in Hungary explained:

> [R]efugees choose iPhones over cheaper alternatives, convinced that investing in a more expensive device would safeguard them from surveillance…. many utilise even multiple devices – like tablets and laptops – each serving a different purpose in their communication strategy. This belief profoundly shapes their preferences; they

> are more cautious about what they share and how they communicate across these devices. For them, choosing a phone or a tablet is not just about functionality; it's about finding a sense of safety in a world where every digital footprint could lead to exposure and potential detention or expulsion.

While in 2018 there was a clear preference for specific iPhones and iPads, this has gradually changed with the awareness of encryption tools of border agencies, pushing more burner phones and multiple devices into border crossing practices. However, a discrepancy remains between those who took action against potential surveillance mechanisms and those who accepted the perceived gaze in their transition countries. Yet, vulnerable migrants should not be underestimated as they are often highly conscious of their digital footprints, routinely monitoring their devices for any signs of surveillance and adjusting their behaviours accordingly. This practice involves reviewing privacy settings, uninstalling potentially harmful apps and managing permissions to prevent unnecessary access to their personal information. Many smartphones, particularly newer Android and Samsung devices, have secure folders that require separate authentication (e.g. a PIN or biometric data) to access. The most tech-literate participants, who also used these phone attributes in their sending countries, employ these to hide sensitive documents, photos or apps from immediate detection in case their phone is searched. In this way, refugees actively shape the boundaries of their technological engagement, ensuring that their digital behaviours do not expose them to increased risks of monitoring or control (Zuboff 2019). However, these measures also make refugees more suspicious to the border authorities.

As has been illustrated, these imaginaries encompass not only the tools of surveillance themselves, but also the beliefs and behaviours that emerge in response to perceived threats. For many refugees, the assumption that they are constantly being watched by migration authorities shapes their understanding of technology and its control over their everyday safety. In transit countries, refugees often resort to unverified social measures to mitigate the risks of surveillance. Some participants emphasised the need for factory reset wipes of all data from the phone, returning it to its original state. This erases any personal information, apps, messages or media that might be used as evidence during a search. Others only said to perform this reset right before crossing borders or checkpoints where phones may be searched. These choices are informed by a collective understanding that technology is intertwined with state power and control, even when the effectiveness of these measures remains unverified. The perception that certain devices or configurations provide a buffer against surveillance becomes a critical aspect of their coping strategies. Some refugees enable full-device encryption, which ensures that the phone's data cannot be accessed without the correct passcode. This is especially helpful in case the phone is seized or stolen, as the data is unreadable without the decryption key.

One of the Syrian participants was told to have copies of his documents – IDs, passports or asylum papers – in secure folders on his Android phone, hidden from authorities during the first inspection. If a phone is searched, the authorities will

not be able to access these files without the necessary credentials. This method is also a result of the media cases of invasive search and inspection of asylum seekers' mobile phones by the Federal Office for Migration and Refugees, which has been legally challenged by GFF.

Software: The invisible mechanisms of control

In contrast, refugees perceive software – such as apps, social media platforms and messaging systems – as abstract and less visible mechanisms of surveillance. While they are aware that software can collect and transmit their data, the opacity of software surveillance often makes it harder for refugees to grasp its full extent, leading to a mixture of anxiety and resignation. This dynamic is particularly evident among refugees who must rely on communication apps like WhatsApp, Facebook and Telegram to stay connected with family and receive critical updates during their journeys. Even though they recognise the risks of data sharing on these platforms, the benefits often outweigh the perceived threats.

Mihaela Nedelcu and Ibrahim Soysüren (2022) describe this as a paradox of digital dependency: refugees are fully aware that these platforms are not secure, yet they are indispensable for communication, navigation and accessing support networks. This reliance creates a cognitive dissonance, where refugees simultaneously engage in self-censorship – such as avoiding sensitive conversations online, using coded language or frequently deleting conversations – while remaining within the dataveillance structures of these platforms. However, the situational diversity of these issues has been hardly explored in this context. According to the interviewees, in a Muslim country they feel far more confident to express their faith than in the EU; however, social and family ties in their home countries would often trigger red flags in transfer countries that are bordering the conflict. One interpreter who had fled Aleppo and was volunteering for an NGO on Lesvos in 2018 explained the affective power of these dynamics:

> We were constantly trying to stay connected while being careful. I still avoid sensitive conversations, use coded language and delete messages often to protect myself. Still, I feel a strong need to rely on others online for support and information. This dependency is tricky; the same tools that help me stay in touch with family and friends also keep me paranoid.

The invisibility of software and the difficulty in understanding its data collection capabilities often lead to more passive forms of self-censorship. Refugees preferably do not modify their use of certain apps, instead developing coping mechanisms, such as switching to encrypted apps (e.g. Signal or WhatsApp) or using features that delete messages automatically after a certain time, or replace written text with voice messages. The details of these coping mechanisms were

also strongly associated with the practices of one's social network, linked to the political region of origin. Unlike hardware, however, which refugees feel they can physically control, the fear surrounding software surveillance is more pervasive and harder to mitigate, creating what Shoshana Zuboff (2019) calls a sense of digital helplessness. As noted earlier, this constantly changing imaginary of control rapidly adjust the norms of connectedness, even when multiple device use continues the common strategy grounded in the visibility of hardware surveillance. Refugees interviewed after crossing the Schengen borders testified about emotional stress and copycat strategies communicated by their travel agents or family networks. Many testified about traveling through high-surveillance areas on the Balkan route after swapping SIM cards, exchanging or flashing their phones (removing all data and resetting the device) before reaching border checkpoints to mitigate the risk of digital surveillance by authorities (Latonero, Kift 2018).

> I try to use different languages in different apps, and even clean up my networks to obscure explicitly sensitive topics. Just try to protect myself while staying connected. Many of us even rely on two phones – one for public use and another for sensitive communications – or change accounts.

The physical manipulation of hardware in order to evade surveillance illustrates the immediacy of the fear associated with these devices. In contrast, during my interviews, participants frequently voiced concerns over social media platforms like Facebook, which they believed were being monitored by both state and non-state actors. Despite recognising the risks, many continued to use these platforms to stay connected with their communities and emphasised the need for critical polymedia use in different settings, i.e. public places, borderlands, private networks or institutional settings. However, they engaged in self-censorship by avoiding politically sensitive topics in their conversations or creating secondary, anonymous accounts in a more affective process (Kappeler, Festic, Latzer 2023). Refugees understand that their mobile software continuously collects data, yet the opacity of how this information is processed and used leads to a more complex form of self-censorship. They may continue using software platforms despite the risks, but engage in subtle behaviours such as coded language or temporary messaging apps, reflecting a form of adaptive disconnection rather than complete evasion. Interestingly, in regions where software censorship is stringent, such as parts of the Middle East, refugees naturally turn to VPNs or proxy servers to bypass software-based surveillance (Casas-Cortes, Cobarrubias, Pickles 2015b). This divergence in digital literacy and trusted technologies illustrates how refugees increasingly perceive hardware as more susceptible to direct interception, while software surveillance is viewed as something that can be evaded through digital tools.

Self-censorship is also strongly defined by the spaces and the places in the mobility path of migrants. Refugees seemed more concerned about hardware at physical border crossings or in highly monitored areas along the Balkan route, and less in places before or after the crossings. At borders, airports or checkpoints, the

physical inspection of phones was more clearly considered a major risk. Especially women thought that their phones could be seized by border authorities, who can access the device's content, photos, messages or apps, which may contain sensitive information about their journeys, personal contacts or even their financial situation. In countries like Turkey, Greece or Hungary, refugees have reported that the authorities search their phones at the borders. While hardware provokes immediate, material responses to mitigate surveillance risks, software elicits more nuanced, sometimes resigned behaviours that reflect both the necessity and danger of digital connectivity, even if they are aware that disconnected devices are also tools to locate them and identify their networks on the move via satellite. Yet, concerns about hardware and software deeply intersect. Crossing Schengen borders illustrates the switch in security concerns, where those who first worried about their physical devices being searched at borders shift to software concerns once they are in safer environments, focussing more on encrypted apps and semantic content of text and voice messages. Forced migrants navigate these fears based on the immediate risks posed by their geopolitical surroundings and the type of surveillance (physical or digital) they socially encounter in those settings. Understanding these imaginaries of risks provides crucial insight into how refugees navigate the digitised landscape of migration daily, illustrating the interplay between visibility, control and agency in their daily digital practices.

Self-censorship strategies as modes of dysconnectivity

The concept of dysconnectivity emerges as a vital lens through which to analyse the self-censorship strategies of refugees carrying connected devices. By choosing to limit their digital interactions by hardware selection, refugees are not merely avoiding surveillance; they are actively disconnecting from or counterfeiting the very technologies that connect them to essential services and social networks.

Dysconnectivity was considered a radical measure, and was only partially used for selective groups or app groups. Fully disconnecting from the internet was reserved for tense situations, like illegal border crossings. However, selections of online presence served multiple roles for the refugees, functioning not only as a communication tool itself, but also as a profiled self-tracker to inform family or as a form of targeted evidence collection in the complex landscape of migration.

> Like this step-tracking app was ok to show my family how far I had travelled. They could see that I was still moving and doing okay. It gave them peace of mind, knowing where I was and that I was safe. The app also kept a record of everywhere I had been, so I could use it if I ever needed to prove where I was coming from.

As self-trackers, these devices allow refugees to monitor their locations, navigate unfamiliar environments and maintain contact with networks of support

in proximity that is also used as a conduit for evidence gathering about their migration trajectory. People on the move regularly repurpose these mobile features, like take photos at different border checkpoints, which are automatically geotagged with location data. These photos serve as proof in their asylum application, showing the route they took and the challenges they faced along the way. Yet, connected tools like smartphones are also repurposed in migration hotspots, and often become a commodity and form of currency within migrant networks, to be sold or used as evidence for migration authorities.

> In Greece some mobile networks allow us to transfer prepaid credit from one phone to another. My brother used this feature to transfer credit in exchange for a taxi ride, but also to get some tools for his work. This is common in areas where you have no cash and people know your situation.

In many cases, refugees use their devices as deposits for financial transactions, selling or trading phones for food, shelter or other essential service, facilitated by local internet shop owners, informal interpreters or travel guides, such as local taxi drivers. In makeshift economies, credit can be traded for other items or services in informal barter exchanges. The ability to communicate is essential, and thus the value of having or being able to provide credit is high. Accordingly, the commodification of mobile technology highlights the duality of these devices: while they facilitate mobility, they also expose refugees to new forms of exploitation and data monetisation. It is well known in the case of Lesvos that free Wi-Fi offered in and around the camp often required users to register with personal information. This data was collected by service providers, leading to potential surveillance and profiling. As Amnesty International indicated, refugees faced increased scrutiny when using these networks. The data generated through the residents' mobile phone use was exploited by various actors, further complicating their relationship with these technologies. As a legal advisor of an INGO emphasised:

> Some humanitarian organisations, like UNHCR, have begun partnering with tech companies to analyse data generated by refugees' mobile usage, offering insights into migration patterns and needs. While this information can improve services, it also raises ethical questions about consent and the potential for misuse. The data harvested can be exploited by various actors – governments, corporations and even malicious entities.

The biometric data collected from migrants are increasingly used to improve machine learning algorithms for private firms, allowing them to enhance facial recognition or fingerprint technology, such as those of IrisGuard. This data is valuable because it often includes individuals from diverse backgrounds, which may be underrepresented in commercial biometric databases. These datasets are also repurposed for commercial products or services unrelated to migration, e.g. smart-doorbells on Amazon. Once companies have developed better algorithms based on migrant data, they can apply these technologies to other sectors – such as banking or retail – for identity verification, which then generates profit. As the famous case

in Jordan's Zaatari refugee camp illustrated, the UN World Food Programme (WFP) implemented iris scan technology to distribute aid to Syrian refugees. While this technology ensures that aid is delivered securely, the collected data were analysed by the companies providing the biometric screening systems. These practices not only fuelled migrants' fear of engaging with digital devices, but in some cases even led to self-mutilation, such as burned fingers and blind eyes to prevent biometric identification protocols. As critical surveillance studies previously warned about such humanitarian surveillance technologies, these companies use the data to refine their software and enhance the accuracy of their algorithmic systems, which are then marketed to other industries such as fintech investing, border security tools or preventive law enforcement measures. Though many refugees would not mind becoming the guinea pig of these investors, they often cannot even provide clear informed consent, because the systems are implemented as a tool in the daily routine of service providers. However, these datafication processes and online registration methods rapidly increased migrants' surveillance awareness, fuelled by myths and misinformation regarding the technology's capabilities and the scope of monitoring by different migration authorities.

Dysconnectivity also gets its way through the selection of hardware. Many participants were advised to wrap their phones in aluminium foil, remove batteries or buy hacking software or tools sold by Amazon to cover their SIM card. With the rise of state-sponsored surveillance and third-party data collection, the choice of communication tools becomes a rhizomic, fluid often intuitive selection of media ecologies, dictated by different beliefs regarding encryption power and the level of privacy offered. For instance, Librem phones are designed specifically with privacy in mind. They run on PureOS, an open-source, Linux-based operating system, and include hardware kill switches to physically disable the camera, microphone, Wi-Fi, Bluetooth or cellular modem to avoid tracking. Similarly, Fairphone, an ethically produced phone that is compatible with LineageOS or /e/OS, was also seen as a tool with a privacy-focussed operating system that provides strong security and limited data tracking. In short, IoT tools and applications were often seen as means of dysconnectivity practices and data security measures by all stakeholders.

Mobile phone application tools of refugees are also often underestimated in their countersurveillance power. Most of the refugees use encrypted messaging apps such as Viber, Signal and WhatsApp, as these platforms offer end-to-end encryption that helps mitigate the risk of surveillance (Leurs, Smets 2018). This preference for encrypted apps reflects an understanding of digital security and an awareness of the vulnerabilities posed by less secure communication platforms, such as SMS or traditional social media applications, which are often more susceptible to interception. Though most participants used these apps interchangeably all the time, refugees in various transit countries disabled their location services on their devices, as another form of self-censorship designed to reduce traceability (Zhang 2023). A volunteer in a Greek NGO explained the practices of their beneficiaries:

> On some phones, you don't even need an extra app to change your location – you can go into the settings, turn on Developer Mode and make it look like you're somewhere else. It's useful when you're trying to stay off the radar. Also, I didn't realise how many apps track your location without you knowing. It's one way to keep control over what they can see.

GPS tracking systems embedded in mobile phones can reveal the user's real-time movements, a significant concern for those attempting to evade border control detection systems. By disabling location features or opting not to use applications that require location data, refugees practice a form of "disconnection" that shields them from being monitored by authorities (Casas-Cortes, Cobarrubias, Pickles 2015b). Some NGO workers claim that most refugees intentionally avoid engaging in social media platforms where their data can be easily accessed and exploited. This choice reflects a broader dataveillance imaginary, where individuals understand the chilling effects of sharing personal information online (Kappeler, Festic, Latzer 2023). For instance, refugees use references to travel agents in the language or holiday service provisions, like referring to "travel agents", "bookings", or "travel guides" when they refer to smugglers in their descriptions. Selective communication represents one of the most immediate and essential strategies of self-censorship among refugees. As de Michel Certeau (1984) suggests, everyday practices often include subtle acts of resistance, and in this context, language itself becomes a tool for evasion.

Refugees often deploy coded language or euphemisms when discussing sensitive topics, such as migration plans or political affiliations, with family members or trusted contacts (Maitland, Xu 2015). By carefully selecting words or using pre-agreed terms that obscure the full meaning of their conversations, refugees reduce the likelihood of detection by surveillance systems that monitor for specific keywords or phrases. In tandem, the practice of limiting what information is shared – whether in direct conversations or via digital platforms – demonstrates a high level of awareness regarding the risks posed by modern surveillance technologies (Latonero, Kift 2018). Refugees often avoid discussing personal details, such as their migration status or their intentions to cross borders, through electronic means. This self-censorship is driven by an acute fear of exposure to state authorities or border enforcement agencies, whose increasing use of surveillance tools has rendered even private conversations vulnerable to interception (Khosravi 2007).

> Which apps we use depends a lot on where we are and who we're talking to. In some places, everyone is on WhatsApp because it's encrypted and trusted, but in others, we switch to Signal or even Telegram if the border control situation changes. It's not just about privacy; it's also about who you can trust on your network.

Also, the selection of communication tools is witnessed as a culturally shaped practice of self-censorship. Refugees often utilise encrypted messaging apps, such as Signal or WhatsApp, over more popular but less secure platforms when their networks preferably use those. Though participants claim that their choice is influ-

enced by a desire for privacy and a heightened awareness of the risks associated with digital communication, their digital tech use is driven by their personal networks, which are fluid and highly influenced by the geopolitical conditions, as well as issues related to religious and class culture (Bastianutti 2024). The anticipatory nature of this self-censorship aligns with the idea that refugees are constructing imaginaries of secure futures based on their experiences of surveillance and control (Schopmans, Ebetürk 2023). Others described how they frequently engage in practices that minimise their digital footprints, such as using unregistered temporary SIM cards, using wearables or registering their devices with fake IDs or even to lost relatives. Additionally, refugees frequently switch SIM cards, disrupting the continuity of tracking mechanisms that rely on stable identifiers (Leurs, Smets 2018). This tactic prevents authorities from associating a specific phone number with an individual over time, thereby complicating efforts to track movement or communication patterns. The ability to remain untraceable in this manner is a form of technological repurposing that reflects refugees' attempts to evade the regulatory and surveillance apparatus designed to monitor their mobility (Scheel 2018).

As Sabina Lawreniuk and Laurie Parsons (2017) argue, refugees engage in a continuous negotiation of their digital and physical presences, seeking to maintain the connections necessary for survival while avoiding the risks of exposure. They emphasise that these technological practices are embedded within the broader context of power, protection and support, illustrating that refugees' engagement with technology is not merely reactive but strategic. The notion of "autonomy of migration" (Casas-Cortes, Cobarrubias, Pickles 2015b) further supports this understanding, recognising that refugees actively reshape their tools to resist the surveillance apparatus and assert their autonomy within the systems that seek to control them.

The falsification of geolocation data also enables refugees to avoid tracking when passing through border zones or other highly monitored areas. By masking their true locations, refugees can evade systems that monitor their communications, preventing governments from identifying or apprehending them.

> When I came to Moria, I learnt how to fake my location on my phone. It's not that hard, and it helps a lot. By showing I was somewhere else, I could keep using the phone without them knowing exactly where I was. I tried to avoid getting flagged by the authorities, who watch everything here.

GPS spoofing apps allow users to manipulate the location data sent by their phone. By using these apps, refugees can make it appear as though they are in a different location. This is especially useful in avoiding detection in monitored zones. These apps are widely available for both Android and iOS devices, and links are shared among different app groups. These tactics also illustrate how refugees navigate the invisible borders of digital surveillance, leveraging sophisticated technologies to subvert state control. These practices not only reflect a tactical approach to evading surveillance, but also illustrate a profound sense of dysconnectivity. By

detaching from stable digital identities, refugees aim to protect themselves from the potential consequences of being identified by state authorities.

This strategy is consistent with the findings of Kiran Kappeler, Noemi Festic and Michael Latzer (2023), which highlight how dataveillance can lead to self-inhibition in legitimate digital communication, fuelling distrust. By utilising GPS tracking features, forced migrants try to navigate routes more effectively and to avoid areas known for heavy surveillance by border authorities. In this sense, mobile phones become instruments of security, enabling refugees to coordinate their movements and prevent disappearance at critical junctures along their journeys. Several INGOs working in outreach and border areas are aware of these techniques and even anticipate them by assisting those who are smuggled in life-threatening crossing points. However, many refugees stated that their choices are often not rational or based on reliable information, but rather follow trial-and-error practices, are chosen under the pressure of smugglers and copycats or are simply from the instructions of others, even via mobile chat groups.

> At the border, you hear a lot of things – some say turn off your phone, others say delete certain apps or chats. Honestly, I didn't always know what was right, so I just tried different things. If someone who made it through said they wiped their phone clean, I did the same. You don't really have a plan; you just follow what others say or what worked for them, hoping it helps you avoid trouble.

Self-censorship practices of refugees regarding their mobile hardware use illustrate complex adaptive strategies rooted in their lived experiences and the influence of telecommunications companies. By engaging in innovative tactics – such as exchanging devices, reprogramming the technology, falsifying IP addresses and leveraging community knowledge – refugees navigate a complex landscape of surveillance while asserting their agency. The role of telco companies and the nature of mobile hardware further complicate this dynamic, emphasising the dual nature of technology as both a tool of empowerment and a potential instrument of control. Understanding these strategies through the lens of techno-authoritarian imaginaries provides valuable insight into the collective perceptions that frame how refugees engage with mobile technology, highlighting the enduring impact of historical and political contexts on their experiences. As one of an exFrontex officer highlighted:

> We've seen refugees adopt some really sophisticated tactics to avoid detection – things like swapping devices, reprogramming their phones, encrypting visual content and using knowledge shared within their communities. It's a constant game of cat and mouse. On the one hand, these technologies empower them to stay connected and to protect smugglers, but on the other hand, they make our job more difficult. We're mainly concerned with criminals like traffickers in our interceptions, but they all seem to fear being suspected as potential terrorists. We rely on a very selective dataset, like telecom companies, but the capabilities of modern smartphones create a situation where technology can either help us enforce the law or be used to bypass it entirely.

While self-censorship may appear as a strategy of disengagement, it also serves as a form of resistance against techno-authoritarian practices. By adopting these modes of dysconnectivity, refugees assert their agency in an environment where their movements and communications are closely monitored. This anticipatory resistance challenges the narrative that refugees are passive subjects of control; instead, they are actively engaging with the technologies at their disposal, even if they are intuitively assessing the risks and benefits of their digital interactions. It has been argued that in high-risk contexts, refugees forgo digital communication altogether, choosing instead to have sensitive conversations in person, away from devices (Leurs, Smets 2018). According to previous digital migration studies, this choice of deliberate withdrawal from digital spaces is not merely a matter of convenience, but a calculated strategy to avoid the traceability associated with mobile phone use. As Zyang (2023) suggest, such forms of "dysconnectivity" reveal the nuanced ways in which refugees negotiate their visibility, selectively participating in digital ecosystems only when it is safe to do so. Still, the analysis of these self-censorship strategies underscores the need for a nuanced understanding of how marginalised populations navigate surveillance infrastructures in terms of psychological and emotional distress. The imaginaries of mobile hardware risks and the perceived role of data sharing practices as securitised devices inform their choices and behaviours, shaping their interactions with digital technologies, the society of local networks and state authorities. This recognition calls for a broader engagement with the practices of future-making, where the implications of surveillance technologies are critically examined in the context of migration (Schopmans, Ebetürk 2023).

Additionally, the shifting dynamics of deportability illustrate how migrants are forced to navigate the spaces between authorised and unauthorised status in different contexts. According to Nicholas De Genova (2002), deportability serves as a defining characteristic of migrant populations, compelling them to constantly adapt their tactics to evade detection and maintain mobility. In this sense, the political nature of migrants' technological practices can be understood as a form of hacking, where they effectively challenge the regulatory frameworks designed to control their movements and limit their agency. By repurposing their hardware and employing digital tools, migrants not only assert their autonomy, but also compel the systems of control to adapt and evolve, thereby reshaping the very nature of migration governance (Casas-Cortes, Cobarrubias, Pickles 2015b; Scheel 2018). This highlights the need for a more nuanced understanding of the situational technopolitics of migrants that acknowledges their ambivalence and organic engagement with technology as a means of navigating and subverting the boundaries imposed upon them.

Adaptive repurposing and dysconnection strategies

The most impressive finding of this study was the scale at which migrants are reprogramming their mobile hardware to enhance privacy and security. These actions reflect both technological agency and an understanding of the vulnerabilities linked to the physical aspects of their devices. While cursive sociotechnical means are often correlated with the internet literacy of digital natives, the market forces of tech tools and peer gadget cultures are deeply underestimated. Refugees manage to install custom firmware or opt for open-source operating systems like LineageOS, which are designed to offer stronger privacy protections. These operating systems provide users with more control over data flows, allowing them to minimise the risks of surveillance tied to pre-installed applications or background services that might collect personal information. This technological customisation allows mobile phone users to exert agency over their devices by removing unnecessary applications that could leak sensitive information. The choice to disable biometric authentication systems, such as facial recognition or fingerprint scanning, is also a deliberate act of self-preservation. These features can potentially expose refugees to additional scrutiny in countries where biometric data is linked to government surveillance systems (De Genova 2013). The reprogramming of hardware becomes not just a matter of enhancing functionality, but a critical act of self-defence against surveillance. As a phone shop owner in Athens explained:

> Look, for a lot of the refugees who come in, messing with their phones isn't just about making them run smoother – it's about keeping safe. In some places, all that biometric stuff can get you flagged by the government, so we help them tweak the settings, turn off tracking or whatever else they need. It's not just tech fixes, it's survival. They're trying to stay off the grid and out of trouble, and this is one way they can do it.

By customising their devices in this way, refugees engage in what Maribel Casas-Cortes, Sebastian Cobarrubias, John Pickles (2015b) term the "autonomy of migration", a concept that highlights the creative strategies migrants use to subvert and resist state control. These modifications are often shared through peer-to-peer networks in Telegram or in simple Facebook or Instagram short videos, which contribute to a collective understanding of how best to safeguard personal data on the move.

To further protect their online presence, refugees frequently employ methods to falsify their IP addresses. For example, refugees may need to access legal rights resources or diaspora communities in their home countries, where websites or forums may be censored or blocked (Nedelcu, Soysüren 2022). Using VPNs allows refugees to bypass these restrictions and communicate securely with family members or access healthcare information. Refugees who fear state monitoring use TOR to avoid being tracked by governments, surveillance firms or other malicious actors (Sadowski 2020).

The falsification of geolocation data also enables refugees to avoid tracking when passing through border zones or other highly monitored areas. By masking their true locations, migrants try to evade systems that monitor their communications, preventing governments and border authorities from identifying or apprehending them. These tactics illustrate how refugees navigate the invisible borders of digital surveillance along the Balkan route, leveraging sophisticated technologies to subvert state control. However, this informal, knowledge-based imaginary of secure device use often contains misinformation or becomes outdated as surveillance tactics evolve. Many of those who learnt in 2016 about secure apps that offer better encryption than WhatsApp or a more secure version of a popular device (ONE) that allows for safer communications (Maitland, Xu 2015) regularly educated themselves in ICT expertise.

> When picking apps and devices, you gotta check out reviews from places like CNET, TechCrunch or The Verge. They talk about security stuff, privacy rules and how users feel. It helps us know what's safe to use, you know?

This form of knowledge-sharing exemplifies a dynamic understanding of technology, where refugees continually adapt their practices based on new information that builds resilience in refugees facing techno-authoritarian systems. Maribel Casas-Cortes, Sebastian Cobarrubias, John Pickles (2015a) refer to these practices as part of the broader "knowledge-based economies of migration", where migrants and refugees capitalise on shared expertise to navigate border regimes, both physical and digital. This exchange of knowledge allows refugees to better manage their digital identities, ensuring that their technology use does not expose them to unnecessary risks. This continuous adaptation, driven by peer knowledge, underscores how refugees remain active participants in shaping their interactions with digital tools.

One of the underestimated aspects of high-tech solutions is their complementary low-tech strategies designed to enhance security and privacy. These strategies demonstrate how refugees blend traditional methods with modern technologies to avoid surveillance risks. For instance, refugees may choose to avoid storing sensitive information on digital devices, instead keeping physical copies of important documents or the other way around. This practice is also perceived as a tool to reduce the risk of interception by authorities, but it is often an unconscious practice, or some even stated that it is culturally embedded in the daily practices of those from authoritarian countries. In particularly high-risk situations, such as crossing borders or navigating hostile environments, refugees may choose to forgo digital communication altogether in favour of in-person conversations. This decision is driven by the understanding that digital interactions can generate traceable metadata and expose them to potential hacking risks, especially when using unsecured networks or devices. For instance, when discussing sensitive topics like their migration journey or legal status, refugees often opt for face-to-face meetings rather than relying on potentially compromised messaging apps. In these contexts,

personal contact becomes more exclusive, as it minimises the risk of surveillance and data breaches. This careful navigation of digital tools and personal interactions reflects a sophisticated awareness of when and how to engage with technology and when to disengage, a practice that scholars refer to as "dysconnectivity" (Zhang 2023). Digital dysconnectivity becomes a deliberate choice, where refugees actively opt out of digital systems when they perceive a heightened threat of surveillance.

Low-tech solutions also include the use of basic phones – devices with limited functionality that lack the extensive surveillance capabilities of modern smartphones. By using these simple phones, refugees minimise the risk of digital tracking, as these devices are less likely to carry spyware or offer avenues for data collection (Leurs, Smets 2018). The decision to use low-tech tools speaks to the broader theme of balancing security with connectivity. Refugees often find themselves in a precarious position, needing to remain connected for survival while also needing to minimise the surveillance risks associated with digital engagement.

Last but not least, we reflect on the role of corporate companies and how their interests shape the counter-surveillance practices of migrants from conflict countries. First and foremost, telecommunications companies and IMEI (International Mobile Equipment Identity) provider companies play a crucial role in shaping the technological landscape that refugees navigate. In many countries, mobile devices are required to be registered using their unique IMEI numbers, which are directly linked to individual users. This system enables authorities to track refugees through their devices, creating significant surveillance risks (Zhang 2023). While they provide essential services, they also contribute to the registration and tracking of mobile devices, which can exacerbate the risks faced by refugees (Elish, Boyd 2017. In response, refugees frequently adopt clever strategies to evade this form of monitoring, including purchasing second-hand phones, using burner phones or frequently changing SIM cards to avoid leaving a traceable digital footprint (De Genova 2013). The proliferation of specific networks as customers in host countries creates a unique connected environment for refugees, as the ambiguous identities associated with these providers and the physical devices – often acquired through informal channels or with false documentation – allow them to navigate technology and surveillance more effectively (Aradau, Perret 2022). The existence of a black market for phones provides refugees with the option to procure devices without personal information attached, circumventing registration requirements that could expose them to danger (Haggerty, Ericson 2006). The same is also valid for phone contracts with providers. Additionally, corporations often emphasise standardised goods and security features of data storage through branding and registration, which influences how refugees engage with technology. The material features associated with corporate branding – such as holograms and barcodes – fuel a sense of legitimacy around mobile devices, even when acquired through less formal means. This duality empowers refugees to leverage the perceived value of these devices while simultaneously engaging in self-censorship practices to protect their identities (Bennett 2010).

Conclusion

Digitised migration processes not only reflect the political and social tensions in different geopolitical contexts, but also shape contemporary power relations between data subjects, migration authorities and humanitarian service providers. This study has critically examined how refugees engage with the imaginaries of mobile hardware technologies in shaping their self-censorship practices within the context of border control surveillance. The research reveals that refugees navigate a multifaceted landscape where the perceptions and realities of technology intersect with the imperatives of survival and identity preservation. The imaginaries associated with mobile hardware and software – shaped by sociopolitical contexts and technological narratives – play a pivotal role in influencing how refugees interact with these tools and manage their digital footprints (Bennett 2016; Elish, Boyd 2017).

The findings highlight that refugees are not merely passive recipients of technology; rather, they actively engage with mobile devices as instruments of agency in a surveillance-rich environment (De Genova 2013). Mobile hardware, often perceived as a means of connectivity and empowerment, simultaneously embodies risks associated with surveillance and data collection. This duality complicates the narratives surrounding technology, wherein the promise of mobility and communication is tempered by the spectre of increased scrutiny and control. Refugees employ a range of self-censorship strategies, including using burner phones, frequently changing SIM cards and opting for in-person communication in high-risk scenarios. These practices reflect a nuanced understanding of the surveillance mechanisms at play, revealing how refugees adapt their behaviours in response to the perceived threats posed by border control authorities (Zhang 2023).

Moreover, the myths surrounding surveillance risks are often amplified by various stakeholders, including telecommunications companies and governmental agencies. While these companies facilitate access to mobile technologies, they also contribute to the surveillance apparatus through the registration and tracking of devices (Haggerty, Ericson 2000). The branding and marketing of mobile technologies often evoke imaginaries of security and connectivity, yet they simultaneously reinforce mechanisms of control that can undermine the safety of refugee populations (Graham 2010). This tension between empowerment and vulnerability illustrates the complexity of refugees' relationships with mobile technology, as they grapple with the dual-edged nature of these tracking tools.

According to the empirical findings presented herein, refugees are not merely passive victims of surveillance, but rather dynamic agents actively navigating the complexities of the technological landscape. The study reveals that the imaginaries surrounding mobile hardware and software features significantly shape the lived experiences of refugees, informing their strategies for navigating an increasingly monitored world. As the digital security landscape continues to evolve, it is imperative for policymakers, scholars and practitioners to consider these complexities in

order to support refugees in their pursuit of safety and dignity, fostering environments that respect their agency and mitigate the risks associated with surveillance technologies. This perspective illuminates the ways in which refugees negotiate their realities, leveraging technology as a means of self-preservation while simultaneously engaging in the practices of dysconnectivity to evade surveillance.

This short reflection aims to challenge the dominant narratives that seek to depict them solely as objects of control, reducing their experiences to mere statistics in the surveillance apparatus of authoritarian regimes. Such oversimplification strips refugees of their tech-savvy resilience and digital agency, masking the sophisticated strategies they employ situationally to reclaim their identities and assert their online autonomy amidst oppressive systems of surveillance (Susser, Roessler, Nissenbaum 2019). By recognising refugees as active participants, we not only explore the different imaginaries of connectedness, but also critically examine the power of self-censorship and expose those who confine connected migrants within frameworks of surveillance authoritarianism (De Genova 2013). This shift in perspective is essential for fostering a more nuanced understanding of migration and technology, highlighting the need to dismantle the stereotypes that perpetuate refugees' tech literacy, and advocating for a more inclusive discourse that acknowledges their capacity for resistance and self-determination.

Declaration of Conflict Interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author received no specific funding for this work.

References

Aouragh M. and Chakravartty P. (2016). 'Infrastructures of empire: Towards a critical geopolitics of media and information studies.' *Media, Culture & Society* 38(4), pp. 559–575. https://doi.org/10.1177/0163443716643007

Bar-Tal D. (2017). *'Self-censorship: The conceptual framework.'* In D. Bar-Tal, R. Nets, and K. Sharvit (eds.) *Self-Censorship in Contexts of Conflict: Theory and Research*. Cham: Springer, pp. 1–18. https://doi.org/10.1007/978-3-319-63378-7_1

Bastianutti L. (2024). *'Digital practices on social media: New perspectives on the production of space and geopolitical inquiry.'* In H. Gülen, C. Sungur, and A. Yeşilyurt (ed.) *At the Frontiers of Everyday Life: New Research in Cramped Spaces*. Cham: Springer Nature Switzerland, pp. 135–153.

Bauman Z. and Lyon D. (2013). *Liquid Surveillance: A Conversation*. Cambridge: Polity Press.

Bennett C.J. (2010). *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge: Mit Press.

Bigo D. (2008). *'Globalized (in)security: The field and the ban-opticon.'* In D. Bigo and A. Tsoukala (eds.) *Terror, Insecurity, and Liberty*. London: Routledge, pp. 3–22.

Bloch A. (2007). 'Methodological challenges for national and multi-sited comparative survey research.' *Journal of Refugee Studies* 20(2), pp. 230–247. https://doi.org/10.1093/jrs/fem007

Campesi G. (2021). *Policing Mobility Regimes: Frontex and the Production of the European Borderscape*. New York: Routledge.

Casas-Cortes M., Cobarrubias S., and Pickles J. (2015a). 'New directions in the study of migration: The autonomy of migration and its implications.' *Antipode* 47(4), pp. 885–895. https://doi.org/10.1111/anti.12157

Casas-Cortes M., Cobarrubias S., and Pickles J. (2015b). 'Riding routes and itinerant borders: Autonomy of migration and border externalization.' *Antipode* 47(4), pp. 894–914. https://doi.org/10.1111/anti.12157

Chen X., Xie J., Wang Z., Shen B., and Zhou Z. (2023). *'How we express ourselves freely: Censorship, self-censorship, and anti-censorship on a Chinese social media.'* In *International Conference on Information*. Cham: Springer Nature Switzerland, pp. 93–108.

Couldry N. and Mejias U.A. (2019). *The Costs of Connection: How Data is colonizing Human Life and Appropriating it for Capitalism*. Stanford: Stanford University Press.

Cupać J., Schopmans H., and Tuncer-Ebetürk İ. (2024). 'Democratization in the age of artificial intelligence: introduction to the special issue.' *Democratization* 31(5), pp. 899–921. https://doi.org/10.1080/13510347.2024.2338852

De Certeau M. (1984). 'Walking in the city.' In M.M. Lock and J. Farquhar (ed.) *Beyond the Body Proper: Reading the Anthropology of Material Life*. Durham: Duke University Press, pp. 249–258.

De Genova N. (2002). 'Migrant 'illegality' and deportability in everyday life.' *Annual Review of Anthropology* 31(1), pp. 419–447. https://doi.org/10.1146/annurev.anthro.31.101401.090029

De Genova N. (2013). 'Spectacles of migrant 'illegality': The scene of exclusion, the obscene of inclusion.' *Ethnic and Racial Studies* 36(7), pp. 1180–1198. https://doi.org/10.1080/01419870.2013.783241

Dekker R., Engbersen G., Klaver J., and Vonk H. (2018). 'Smart refugees: How Syrian asylum migrants use social media information in migration decision-making.' *Social Media + Society* 4(1). https://doi.org/10.1177/2056305118764439

Deleuze G. (1992). 'Postscript on the societies of control.' *Cultural Theory: An Anthology*, pp. 139–142.

Elish M.C. and Boyd D. (2017). 'Situating methods in the magic of Big Data and AI.' *Communication Monographs* 85(1), pp. 57–80. https://doi.org/10.1080/03637751.2017.1375130

Falzon M. (2012). *Multi-Sited Ethnography: Theory, Praxis and Locality in Contemporary Research*. London: Routledge.

Fenwick T. (2015). *'Sociomateriality and learning: A critical approach.'* In D. Scott and E. Hargreaves (eds.) *The SAGE Handbook of Learning*, Los Angeles: SAGE, pp. 83–93.

Filak V.F. (2010). 'Self-interest, the common good and a sense of purpose: Examining precipitating factors of the willingness to self-censor.' *College Media Review* 47(3–4), pp. 24–30.

Gerhold L. and Brandes E. (2021). 'Sociotechnical imaginaries of a secure future.' *European Journal of Futures Research* 9(1), pp. 1–12. https://doi.org/10.1007/s40309-021-00223-2

Gillespie M., Osseiran S., and Cheesman M. (2018). 'Syrian refugees and the digital passage to Europe: Smartphone infrastructures and affordances.' *Social Media + Society* 4(1). https://doi.org/10.1177/2056305118808821

Gonzalez S.M. and Deckard F.M. (2024). '"We got witnesses" black women's counter-surveillance for navigating police violence and legal estrangement.' *Social Problems* 71(3), pp. 894–911. https://doi.org/10.1093/socpro/spac043

Hage G. (2005). 'A not so multi-sited ethnography of a not so imagined community.' *Anthropological Theory* 5(4), pp. 463–475. https://doi.org/10.1177/1463499605057834

Haggerty K.D. and Ericson R.V. (2006). *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

Haile Y.R. (2021). 'The liberalities and tyrannies of ICTs for vulnerable migrants: The status quo, gaps and directions.' *arXiv*. https://doi.org/10.48550/arXiv.2108.09782

Hennink M.M., Kaiser B.N., and Weber M.B. (2019). 'What influences saturation? Estimating sample sizes in focus group research.' *Qualitative Health Research* 29(10), pp. 1483–1496.

Hesselberth P. (2018). 'Discourses on disconnectivity and the right to disconnect.' *New Media & Society* 20(5), pp. 1994–2010. https://doi.org/10.1177/1461444817711449

Kappeler K., Festic N., and Latzer M. (2023). 'Dataveillance imaginaries and their role in chilling effects online.' *International Journal of Human–Computer Studies* 179. https://doi.org/10.1016/j.ijhcs.2023.103120

Kazansky B. (2021). "It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance.' *Big Data & Society* 8(1). https://doi.org/10.1177/2053951720985557

Kerezsi K. and Nagy V. (2020). *A Critical Approach to Police Science: New Perspectives in Post-Transitional Policing Studies*. The Hague: Boom Uitgevers Den Haag.

Khosravi S. (2007). 'The 'illegal' traveller: An auto-ethnography of borders.' *Social Anthropology/Anthropologie Sociale* 15(3), pp. 321–334. https://doi.org/10.1111/j.0964-0282.2007.00019.x

Khosravi S. (2017a). *After Deportation: Ethnographic Perspectives*. New York: Palgrave Macmillan.

Khosravi S. (2017b). 'Precarious lives: Waiting and survival in the United States and Europe.' *The Sociological Review* 65(5), pp. 858–876. https://doi.org/10.1177/0038038517696642

Latonero M. and Kift P. (2018). 'On digital passages and borders: Refugees and the new infrastructure for movement and control.' *Social Media + Society* 4(1). https://doi.org/10.1177/2056305118764432

Lawreniuk S. and Parsons L. (2017). 'The politics of migrant mobility: Power, protection, and support.' *Journal of Ethnic and Migration Studies* 43(3), pp. 365–383. https://doi.org/10.1080/1369183X.2017.1349463

Leese M. (2022). 'Fixing state vision: Interoperability, biometrics, and identity management in the EU.' *Geopolitics* 27(1), pp. 113–133. https://doi.org/10.1080/14650045.2020.1830764

Leurs K. and Smets K. (2018). 'Five questions for digital migration studies: Learning from interdisciplinary dialogue on migration, media and communication.' *Social Media + Society* 4(1). https://doi.org/10.1177/2056305117753940

Lock M.M. and Farquhar J. (eds.) (2007). *Beyond the Body Proper: Reading the Anthropology of Material Life*. Durham: Duke University Press.

Lyon D. (2010). *'Surveillance, power and everyday life.'* In P. Kalantzis-Cope and K. Gherab Martín (eds.) *Emerging digital spaces in contemporary society: Properties of technology*. London: Palgrave Macmillan UK, pp. 107–120.

Maitland C. and Xu Y. (2015). 'A social informatics analysis of refugee mobile phone use: A case study of Za'atari Syrian refugee camp.' *TPRC 43: The 43rd Research Conference on Communication, Information and Internet Policy Paper*. https://dx.doi.org/10.2139/ssrn.2588300

Marcus G.E. (1995). 'Ethnography in/of the world system: The emergence of multi-sited ethnography.' *Annual Review of Anthropology* 24(1), pp. 95–117.

Miellet S. (2021). 'From refugee to resident in the digital age: Refugees' strategies for navigating in and negotiating beyond uncertainty during reception and settlement in the Netherlands.' *Journal of Refugee Studies* 34(4), pp. 3629–3646.

Milivojevic S. (2021). *Crime and Punishment in the Future Internet: Digital Frontier Technologies and Criminology in the Twenty-First Century*. Abingdon: Routledge.

Milivojevic S. and Biles J. (2017). 'The paradox of border security: Migration, surveillance, and resistance.' *Critical Criminology* 25(2), pp. 197–215. https://doi.org/10.1007/s10612-016-9354-5

Minca C. and Collins J. (2021). 'The Game: Or 'the making of migration' along the Balkan Route.' *Political Geography* 91(1). https://doi.org/10.1016/j.polgeo.2021.102490

Morgan H. (2023). 'Living digitally like a migrant: Everyday smartphone practices and the (Re)mediation of hostile state-affects.' *Progress in Human Geography* 47(3), pp. 409–426. https://doi.org/10.1177/03091325231174311

Nagy V. (2024). 'The risks of data litter in contemporary policing cultures: Interrogating data sharing between humanitarian NGOs and the Public Security

Agencies.' In T. Østbø Kuldova, H.O.I. Gundhus, and Ch.T. Wathne (eds.) *Policing and Intelligence in the Global Big Data Era. Volume II: New Global Perspectives on the Politics and Ethics of Knowledge*. Cham: Springer Nature Switzerland, pp. 159–194.

Nalbandian L. (2022). 'An eye for an 'I:' a critical assessment of artificial intelligence tools in migration and asylum management.' *Comparative Migration Studies* 10(1). https://doi.org/10.1186/s40878-022-00305-0

Nedelcu M. and Soysüren I. (2022). 'Precarious migrants, migration regimes, and digital technologies: The empowerment-control nexus.' *Journal of Ethnic and Migration Studies* 48(8), pp. 1821–1837. https://doi.org/10.1080/1369183X.2020.1796263

Ozkul D. (2023). *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe*. Oxford: University of Oxford.

Pallister-Wilkins P. (2022). *Humanitarian Borders: Unequal Mobility and Saving Lives*. London: Verso Books.

Petit N. (2020). *Big Tech and the Digital Economy: The Moligopoly Scenario*. Oxford: Oxford University Press.

Pfeifer M. (2021). 'Intelligent borders? Securitizing smartphones in the European border regime.' *Culture Machine* 20, pp. 1–22.

Pink S., Ardèvol E., and Lanzeni D. (2020). *'Digital materiality.'* In S. Pink, E. Ardévol, D. Lanzeni (eds.) *Digital Materialities: Design and Anthropology*. Abingdon: Routledge, pp. 1–26.

Rayes A. and Salam S. (2022). *Internet of Things From Hype to Reality: The Road to Digitization*. Cham: Springer International Publishing.

Sadowski J. (2020). *Too Smart: How Digital Capitalism is Extracting Data, Controlling our Lives, and Taking over the World*. Cambridge: MIT Press.

Sánchez-Querubín N. and Rogers R. (2018). 'Connected routes: Migration studies with digital devices and platforms.' *Social Media + Society* 4(4). https://doi.org/10.1177/2056305118808821

Scheel S. (2018). 'The autonomy of migration: A new framework for understanding the politics of mobility.' *Geopolitics* 23(1), pp. 110–127. https://doi.org/10.1080/14650045.2017.1342243

Scheel S. and Ustek-Spilda F. (2019). 'The politics of expertise and ignorance in the field of migration management.' *Environment and Planning D: Society and Space* 37(4), pp. 663–681.

Schopmans H. and Tuncer-Ebetürk I (2024). 'Techno-authoritarian imaginaries and the politics of resistance against facial recognition technology in the US and European Union.' *Democratization* 31(5), pp. 943–962. https://doi.org/10.1080/13510347.2023.2258803

Susser D., Roessler B., and Nissenbaum H. (2019). 'Technology, autonomy, and manipulation.' *Internet Policy Review* 8(2). https://doi.org/10.14763/2019.2.1410

Tanczer L.M., Deibert R.J., Bigo D., Franklin M.I., Melgaço L., Lyon D., and Milan S. (2020). 'Online surveillance, censorship, and encryption in academia.' *International Studies Perspectives* 21(1), pp. 1–36. https://doi.org/10.1093/isp/ekz016

Trauttmansdorff P. (2022). 'Borders, migration, and technology in the age of security: Intervening with STS.' *Tecnoscienza–Italian Journal of Science & Technology Studies* 13(1), pp. 51–69. https://doi.org/10.33679/tec-2022-1951

Učakar T. (2020). 'The rhetoric of European migration policy and its role in criminalization of migration.' *Causes and Consequences of Migrant Criminalization* 81, pp. 91–108. https://doi.org/10.1007/978-3-030-43732-9_5

Wahlberg A. (2022). *'Assemblage ethnography: Configurations across scales, sites, and practices: post-structuralism.'* In M. Hojer Bruun, A. Wahlberg, R. Douglas-Jones, C. Hasse, K. Hoeyer, D. Brogård Kristensen, and B.R. Winthereik (eds.) *The Palgrave Handbook of the Anthropology of Technology*. Singapore: Springer Nature Singapore, pp. 125–144.

Wang Y., Ahmed S., and Bee A.W.T. (2024). 'Selective avoidance as a cognitive response: examining the political use of social media and surveillance anxiety in avoidance behaviours.' *Behaviour & Information Technology* 43(3), pp. 590–604. https://doi.org/10.1080/0144929X.2023.2182609

Zhang G. (2023). 'Mobile media in China: Media practice as a research orientation.' *Mobile Media & Communication* 11(1), pp. 80–87. https://doi.org/10.1177/2050157922113494 7

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

Zureik, E., Stalker, L. H., Smith, E., Lyon, D., & Chan, Y. E. (2010). *Surveillance, privacy and the globalization of personal information*. Montreal: McGill-Queen's University Press.