## What harms may come?

*Exploring the anticipatory dimensions of surveillance resistance in an age of datafication*

Kazansky, B.

**Publication date**
2021

# Chapter 8:[21] Preventing Preemption: Exploring 'proactive' strategies to counter anticipatory surveillance regimes

21 This chapter has been submitted for peer review in July, 2021

# Abstract

This chapter explores how preemptive surveillance is countered, interrupted, and co-opted by targeted communities in their daily work and organizing strategies. Drawing on findings from a four-year qualitative study of resistance to surveillance amongst transnationally networked NGOs and grassroots groups, the chapter constitutes an empirical and theoretical exploration of the imperative for affected communities to *proactively* act *before* violent preemptive surveillance driven measures can exert harmful effects. The chapter investigates how the orientation towards proactivity influences security/safety practice and community organizing work, looking particularly at the proactivity of data-driven *resilience* and abolitionist *refusal* in human rights and social justice organizing work. The analysis of proactivity – defined here as the imperative to act before probable harm from preemptive violence – provides insight into the potentials of resistance to what Mackenzie calls an 'anticipatory regime' (Mackenzie, 2013) of contemporary surveillance and policing.



**Keywords:** predictive policing, preemption, abolition, refusal, resilience, digital security, automated systems, temporality

# Introduction

'Before the bullet hits the body' is the title of an incisive research report published by the grassroots US abolitionist group STOP LAPD Spying Coalition (SLSC)[22]. The report breaks down the problematics of predictive policing in Los Angeles and pushes for the urgent abolition of the 'Stalker State' (STOP LAPD Spying Coalition, 2018). The title of the report, according to an interviewed community organizer and volunteer, emerged from the many meetings during which the group worked through strategies to support poor, unhoused, immigrant, Brown and Black communities put at the sharp edge of oppressive policing measures in Los Angeles. Since 2010, the city of Los Angeles has been a central site of contestation around the harms of predictive policing (Brayne, 2017; 2020), a paradigm of policing characterized by the use of data-driven techniques to preemptively surveil suspected individuals, communities, and their surrounds (Andrejevic 2017; Petty et al., 2018; Williams, 2019). Responding to the automated forms of preemption at play in the 'intelligence-led policing' programs of the Los Angeles Police Force, the title of the SLSC report has a dual meaning. First, it refers to the police force's imperative to preempt criminality through actions that have resulted in well-documented cases of policing abuse. Second, it refers to the SLSC's urgent imperative to prevent further harm to its constituent communities at the hands of the police. Reflecting on the work entailed in countering the harms of preemptive surveillance in Los Angeles, the volunteer organizer explained that saving lives within an environment punctuated by danger and repeated loss meant 'acting

22 LAPD stands for the Los Angeles Police Department

proactively...realizing that my fight wasn't just the aftermath but the before' (Interview #43).

This chapter explores the 'before' and its spatial-temporal logics as the site of contestation around preemptive regimes of surveillance. The 'before' or the 'not yet' (Dencik et al., 2018) is a 'time/space of preparedness'(Aradau and van Munster, 2012). 'Acting on the time before', writes Massumi (2015: preface) is the 'operative logic' of violently preemptive actions taken by powerful actors (viii). While the existing literature focuses on the actions of policing and security actors, SLSC's work organizing against predictive policing harms shows that countering the harms of preemptive action also implies 'acting on the before' – to disrupt what Sheehey (2019) characterizes as the paranoid and racialized temporality of policing. The before, per the interviewed SLSC organizer, is a vital pocket of indeterminacy and a buffer against the violent injunction of systems which aim to control and narrow future(s), which must be harnessed and defended by communities through 'proactive' strategies of safety. Looking beyond the experiences of SLSC, the need to act *proactively* against anticipated surveillance and data-related harms is a central theme arising in the interviews and field work conducted in my four-year study of surveillance resistant practices and infrastructures in the context of civil society and social movement efforts to advance the cause of data justice[23].

23 In this chapter, 'civil society' and 'movements' are terms used describe how the people who are featured in this chapter respectively describe their communities. While interrelated and often overlapping, the groups and individuals interviewed here often make a meaningful distinction between the NGO-driven work of transnational civil society and local, grassroots, movement-based organizing. These distinctions adhere to differing political commitments and degrees of institutionalization. For clarity, 'civil society' refers to a global field of transnationally coordinating digital security experts, technologists, and

Drawing on my findings from this study, the chapter provides an account of the imperative for affected communities to proactively act *on the time before* preemptively violent surveillance measures can exert harmful effects. This exploration of proactivity is intended to shed light on possibilities to challenge preemptive logics and anticipatory regimes. The chapter sits in dialogue with scholarly work on data justice, resistance to surveillance, and agency in a datafied society (Benjamin, 2019; Browne, 2015; Dencik, et al., 2019; Gangadharan, 2020; Milan and van der Velden, 2016; Van Dijk, 2014). Scholars studying these issues argue that what requires more attention is how different social groups can and do already intervene into the preemptive and predictive logics that suffuse contemporary surveillance and data-driven systems (Andrejevic et al. 2019; Gangadharan, 2020; Minocher and Randall (2020). The goal of this chapter is to contribute to this growing body of literature by exploring the preconditions and ambiguities of resistance to preemptive surveillance. 'Proactive' action is often framed as a future-focused orientation tied to a capacity for foresight and agency. In the context of policing, proactivity refers to data-driven preemption. In the context of activism, proactivity may refer to positive co-optations of data for social good, highlighted as examples of empowerment and agency. This chapter adds a new dimension to understandings of proactivity in relation to policing, activism, social movements, and civil society, re-contextualizing proactivity to mean an imperative to act before probable harm is caused by violently

NGOs involved in 'internet freedom' and digital rights, while the 'movements' at play are the grassroots community organizers and their constituent communities in Los Angeles, in the United States. In exploring efforts to resist and counter preemptive surveillance, the chapter explores the meeting points and divergences of civil society actors and movement based community organizers, noting both their common goals and differences.

preemptive actors. The chapter investigates how this form of proactivity is embodied and enacted when imbricated within the security/safety practices of human rights defence and social justice organizing work. The relationship between preemption and proactivity is explored through two cases drawn from ethnographic field work around transnational digital rights and Internet freedom communities that develop technical counter-measures for security and surveillance, and fight for different notions of justice and rights in relation to technology and society.

The plan of the chapter is as follows: in the next section, I contextualize my concern with proactivity and strategies to counter preemptive logics, drawing on literatures relating to policing, surveillance, and activism and social movements. Following, I discuss my methods and research positionality. Then I introduce the two empirical cases of the chapter, each serving to highlight the importance of proactivity in the context of resistance to preemption. The first case explores resilience as enacted through structured security protocols in the context of a digital security exercise conducted to prepare for preemptive office raids of human rights organizations by state actors. The second case looks deeper at the efforts of the SLSC to challenge the carceral logics and practices of predictive policing in Los Angeles through the collective refusal of abolitionist community organizing. The chapter concludes with a critical discussion of empowerment and agency vis a vis the imperative to act proactively against preemptive harms.

# Preemption, proactivity, and empowerment

This chapter explores how preemptive logics are countered in two different settings. In both, the chapter identifies and explores an orientation towards proactivity and the seizure of the spatio-temporal 'not yet' as a locus point between violent state security apparatuses and social movements defending their autonomy and lives. Whereas the 'proactive', orientation of policing has been explored extensively in criminological and security literature, this chapter explores 'proactivity' within actions taken to resist, contest, or find safety amidst violent anticipatory regimes. This section of the chapter does two things: first, it provides a short overview of preemptive surveillance and policing and contextualizes proactivity in relation to literature. Second it looks at proactivity in relation to resistance to preemptive measures, community organizing, and contemporary activism.

In the context of surveillance, security and policing, preemption implies the will (and power) to forcefully intervene against undesired futures. In practice, the ability to act preemptively implies the use of violence to foreclose the futures of people deemed risky or undesirable to powerful institutions and actors (Andrejevic, 2020; Benjamin, 2019; Browne, 2015; Wang, 2018; Williams, 2019). Preemptive security and surveillance do not by definition imply the use of big data, nor are they 'new' phenomena (c.f. van Brakel, 2016). Preemptive actions such as raids, arrests have been a long-standing concern for social movements (Gillham, 2011; Porta et al., 2006). Further, preemption has been explored extensively as a political ideology driving counter-terrorist actions by states after 9/11 (Amoore, 2013; Anderson and Adey 2011; de Goede, 2008; 2009; 2014; Suchman, 2017; 2020). Dencik et al. (2015; 2018) and

Gillham (2011) highlight preemptive measures such as preemptive arrests, the disruption of protests through checkpoints and searches, and 'kettling' (Swain, 2013) in order 'to isolate and contain disruptive protesters whether actual or potential' (Gillham, 2011: 637, in Dencik et al., 2018). These kind of preemptive actions do not necessarily depend on the use of digital, big data-driven surveillance per se, however, the use of different forms of adversarial information collection and intelligence is essential, and can be understood as part of an unfolding history of 'Intelligence-Led Policing (ILP) (Browne, 2015; De Hert and Vis 2005; Van Brakel, 2016).

Per the SLSC (2018), ILP has 'oriented law enforcement towards activities of data gathering, data analysis, and preemptive action against presumed criminal and terrorist activity'(4). Scholars from across criminology, security studies and surveillance studies characterize intelligence-led policing as part of a shift from 'reactive' to 'proactive modes of action in policing, constituting a 'turn' to proactive modes of 'disciplinary power' (Andrejevic, 2020: 87). Broadly, the term 'proactive' in this context is used to characterize the intwining of data-driven techniques and future-oriented temporal logics (Bigo, 2006; Brayne, 2016; Dencik et al., 2017; Massumi, 2015). Per Dencik et al. (2017), the 'transformation from 'reactive' to 'proactive' policing combines data analysis with human intelligence and interpretation' (pp.1146). It is in this longer trajectory in 'proactive' punitive and violent state action that novel predictive policing techniques and platforms have been promoted and sold to police departments around the world. 'Big' data and data-driven policing platforms augment and propel the preemptive logics of ILP in new ways, entrenching a longer move towards quantitative and statistical methods of policing (Didier, 2018). Andrejevic et al. (2019) characterize the logic of predictive policing as a 'just-in-time'

temporality premised on preempting an event just before it happens, 'so there is sufficient evidence to detain or arrest, but the crime itself is averted.'(3). This is a defining element of 'the compressed temporality of preemption, which simulates an anticipated future in the present so as to act upon it before it can occur' (Andrejevic, et al., 2019: 4) in order to 'optimize the precious time that police forces have'(Funnell, 2015 quoted in Andrejevic, 2020: 86).

In the section above, I contextualized the notion of 'proactivity' in relation to policing, a context in which proactivity is a violent, time-bound and data-driven orientation growing out from histories of racist oppression, carceral institutions, techniques of war, and an intensified surveillance society. Here I highlight that proactivity also arises as a theme in studies of contemporary activism, signifying a form of empowered use of data. 'Proactive data activism', as coined by Milan (2016) and further explored by Gutiérrez and Milan (2019) relates to efforts by 'data activists' to exploit the new availability of 'big data' in support of varied notions of social good. Data-intensive projects such as Ushahidi and other participatory mapping projects are explored as positive co-optations of dominant logics and potential portals to alternate imaginaries of datafication. Within this heuristic, proactive data activism is contrasted with 'reactive' data activism, which refers to efforts to resist surveillance and datafication, including through safety and security practices. Considering that this chapter's concern is with safety and security, the 'proactive' actions explored in this chapter do not neatly align with the data activist proactive/reactive heuristic. Rather than referring to the exploitation of available data towards 'positive' activist ends such as those described above, proactivity in this chapter refers to a temporal orientation which emerges within the imperative to urgently prevent or mitigate harms caused by the

intersections of surveillance, carceral technologies and oppressive preemptive actions. That being said, I will later show that in the context of security practices, the 'proactive' orientation towards future harm can lend itself to data-driven action, as in the first case of this chapter, which explores civil society's turn to data-driven resilience in security. In contrast, in the second case, proactively arises within the abolitionist refusal to engage with or be captured by data and its underpinning logics all-together. This tensions between resilience and refusal, and how the use of data figures into these two strategies, is explored in subsequent sections of the chapter. For now, I end this section of the chapter with a question. Having noted that proactivity comes into play for both violent, preemptive actors and, consequently, their subjects, it is worth asking to what degree proactivity always implies empowerment, and if it does, is this the kind of 'empowerment' that is invoked in the positive sense of the word with regards to 'proactive data activism'? This is a question I return to later.

# Methods and research positionality

This chapter draws on data from 50 interviews and participant observation field work conducted with NGO staff, human rights defenders, digital security specialists, and social justice organizers working with communities affected by surveillance between 2016 and 2019. The selection of interviewees resulted from purposeful sampling at 12 international meetings and conferences devoted to promoting Internet freedom, digital rights, digital justice, and social justice in Europe and Southeast Asia. Interviewees come from 26 countries, a result of the demographics of the gatherings where

fieldwork was done, which are representative of the transnational nature of the larger field concerned with issues around human rights, social justice, and technology. This field is comprised of heterogenous communities with oft-conflicting politics (c.f. Mouffe, 2013; Horgan and Dourish, 2018), which nonetheless coalesce at international events to discuss common threats, shared values, and to establish consensus – where possible – on 'best practices' around digital security, digital rights, and related issues. This chapter draws on these interviews and participant observation for its analysis of proactivity, a theme discussed across the heterogeneous communities interviewed in my research. The two cases featured in this chapter highlight two particular contexts of human rights and social justice work, where the actors above contend with preemptive measures through different forms of resistance and contestation. The first context explored is an international training bringing together people from the human rights defender community from all over the world to develop security preparedness protocols. The second context concerns the work of STOPLAPD Spying Coalition, looking in particular at a conversation staged by the organization at a digital rights conference in Europe, where they about how to counter the harms of predictive policing. In this chapter, all interviewees and the groups they work with have been anonymized due to safety concerns. Certain organizational names remain, with their consent.

A note on my research positionality: inspiration for this chapter comes from my own background of practice in the field of digital security and safety for human rights and social justice, during which time I worked with different NGOs and grassroots groups to understand how to connect matters of safety and security to broader movement goals (Kazansky, 2015; 2016). Throughout my years engaging in this work, tactics and strategies employed towards the

goal of safety underwent continued iteration and contestation amongst security practitioners and the groups they worked with to devise strategies for safety and security (as I document in Kazansky, 2021 and Kazansky and Milan, 2021). During my time as a digital security practitioner, I often encountered boundary conflicts around what constitutes effective 'individual' and 'collective' action as it pertains to self-defence and community defence; an observed disillusionment with technical 'solutions' to surveillance; increased efforts to grapple with racism, neo-coloniality, carceral logics, and diversity issues within the field itself, and the continued re-configuration of pedagogical practices to help groups imagine and prefigure just futures. As the issues highlighted above have made their mark on digital security practice within transnational civil society, digital security practitioners have reflected on how the practices they promote and teach can better support the goals of the grassroots groups and movements which they engage with. It is in this spirit of this weighty responsibility that I engage in this chapter with the unjust histories and practices of preemption and the vital contributions of abolitionist thinking and organizing to social justice, as it is now advanced by STOPLAPD Spying Coalition and other groups highlighted in the chapter.

## The proactivity of *security preparedness protocols*

> "For people to make time for security is really difficult. Every day there are so many immediate threats that need to be handled and the work never stops unless someone is dead or

> has experienced some breakdown. People react to immediate threats and the challenge is to get them to think about long term planning, strategy, to have a policy in place before things happen, and to be proactive instead of reactive" (Interview #6).

This quote is from a digital security trainer who teaches security countermeasures to international human rights nonprofits and grassroots groups across different regions of the world. His repertoire as a trainer addresses a spectrum of technologically related security incidents of concern, from suspected computer compromise, to online harassment and defamation campaigns by state sponsored actors. As his experience indicates, the challenges of human rights work require making time for security before insecurity forecloses time. He emphasizes that human rights defenders must be 'proactive' lest they overtaken by harm. But what does it mean to be proactive in the context of security practices for human rights work? This was a central subject of discussion at an observed training taking place in 2018. This section of the chapter explores the site of this digital security training as a liminal space constructed to help those concerned with safety harness the 'tensed time-space where disaster is not-yet, action is demanded, decisions are weighted with consequence, and action is animated by necessity and urgency' (Anderson and Adey, 2011: 1102). The vignette in this section positions the training as a jumping-off point to explore how the security protocols are taught in order to mitigate potential harms of digital threats. As part of this exploration, I look at how these security protocols are productive of a particular regime of resilience and 'resilient subject' (O'Malley, (2010).

The training, staged in a quiet European city by a long-established human rights organization working at a transnational level, brought together a group of 20 self-described human rights defenders[24] (HRDs) from 16 countries to learn practical security countermeasures. A number of HRDs arrived seeking reprieve from urgent concerns, working with families of the desaparecidos in Mexico; with LGBTQIA+ activists in Nigeria; with digital rights organizations in Tunisia; and with women's rights activism in the Philippines[25]. Taking place over five days, the event comprised three educational modules divided into topics of security from a digital, physical, and 'psychosocial' perspective. On the table were everyday data issues affecting non-profit organizations and grassroots initiatives: digital device failure, data theft, commercial data exploitation, as well as concerns particular to human rights work: preemptive office raids by local police and national security agencies; targeted attacks on high-profile HRDs; the wiretapping and digital monitoring of movements' online activity and violence against women online and 'offline'.

After several days of software demonstrations of security counter-measures such as password management software and encrypted email, the participants were asked to synthesize 'learnings' through

24 The term 'human rights defender' is common to the international human rights community, used to describe and legitimize the work of individuals engaging in a number of different forms of activism. The status of human rights defenders as people and groups deserving protection has been legitimated through UN processes such as the United Nations Declaration of Human Rights Defenders (1998). See: http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Declaration.aspx and 'Who is a defender?': http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Defender.aspx.

25 Names and other identifying details have been changed

engagement in a speculative scenario planning exercise. Sitting together in a circle, the trainer asked the group to imagine that an office raid was about to occur at a hypothetical non-profit civil society organization. Office raids have been well-documented in the international human rights community in recent years, with an observed increase tied in part to a string of new national security laws implicating human rights organizations as 'foreign agents' or actors in countries such as Russia and India (Amnesty International, 2017). As human rights organizations document, vague suspicions of foreign influence are invoked to justify a raid (Elder, 2013; Human Rights Watch, 2020). During a raid, police or security actors may grab paperwork, seize or destroy digital devices and threaten physical intimidation, justifying these actions on the suspicion that the civil society organization has broken the law tInformation exfiltrated through the raid is then used to build a legal case against the organization and used as grounds to shut down an organization's operations. To gather the greatest quantity of compromising or incriminating information requires catching the organization unprepared. Thus office raids must be planned to take place 'just in time'(c.f. Dencik et al. (2017) in order to maximize the element of surprise. The digital security trainer leading event observed that raids often follow on a period of digital or physical monitoring of organizational infrastructure to identify potential weaknesses and vulnerabilities in their work and technology. This kind of preemptive scanning of organizational vulnerabilities enables the party planning the raid to determine the best moment for the execution of preemptive action.

'An office raid is imminent. What should be done to prepare?' On a white board, the security trainer asks the participants to break down potential mitigations into two columns: 'reactive' and 'proactive'.

‘Reactive’ connotes actions taken in the immediate wake of an emergency event, digital or physical. ‘Proactive’ refers to preparations that could be made ahead of time in anticipation of probable threats. In the reactive column participants add suggestions such as ‘keeping calm’ ‘staying vigilant’ and ‘sending an SOS message to a colleague’. One participant notes a dilemma: amidst the urgency of an office raid, there might not be enough time to reach out to a colleague for help. Hence, it is deemed essential by the training participants to ‘know beforehand who to turn to if you need money or technical support’(field notes, 2018). If receiving assistance in the middle of an emergency requires time that’s not there for the taking, processes should be set in place beforehand in anticipation of problems, argues the trainer, as though, per Adams et al, (2009), ‘the event and the trauma...were already here’(257). When this emergency inevitably occurs, there will not be the time or space for deliberation to determine how to best respond. This implies that security and safety is only be possible if HRDs can match the ‘just in time’ tempo of preemptively threatening actors and perpetrators of violence through structured preparedness protocols.

The training participants thus discuss the need to put in place a spokesperson or ‘lifeline’ ahead of time in order to increase the chance of being able to contact them in the midst of the hypothetical emergency. In the proactive mitigation column, participants write: ‘select a spokesperson, have a lifeline, monitor the context, check the local law’. The digital security trainer of the training suggests that a proactive mitigation could also include the creation of data backups in anticipation of its loss (a practice highlighted by pink et al. (2018) as an example of an ‘anticipatory mode’ of data practice, which I further expand upon in Kazansky (2021). Added to the growing ‘proactive’ column are: the installation of CCTV cameras around the

office, the duplication and back up of sensitive data at a separate location, regular software updates to patch software vulnerabilities, and the use of digital firewalls against unwanted digital intrusions into networks and computers.

This enumeration of proactive and reactive actions exposes a tension in the temporal scaffolding of proactivity. What, a participant asks, is the moment at which an action should be designated as proactive? For example, if an organization begins backing up its data following a cyberattack or office raid, does that make the back up a reactive or proactive measure? On the one hand, the measures are implemented in response to an event. On the other hand, the measures are intended to prevent or mitigate the effects of future events. Though the reactive and proactive have been delineated as dichotomous, the leveraging of past experiences to inform future-oriented action shows that proactivity piggybacks on reactivity. To put it differently, the logic of proactivity harnesses an individual or community's experience of past harm to 'prime' itself (Massumi, 2015) for potential future threats. As the discussion in the security training shows, To take back time for security (as encapsulated in the elusive 'before') means to optimize for efficiency and engage in a temporal dance constructed by powerful actors to elude perception by their targets.

Further, as made evident in the above discussion, to 'proactively' intervene into a preemptive event is tricky, and its prevention is not always deemed possible. Due to the continuous threat of temporal foreclosure through preemptive digital compromise or violence, the trainer stressed a need to act in a more structured and efficient mode; to 'build standard operational procedures for the daily of human rights work' (Interview #39). This raises the question: what happens

to ‘the before’ when there is not a singular event to prepare for, but a spectrum of violent potentiality ‘not yet emerged’ (Dencik et al, 2018: 1435)? What sorts of commitments (and burdens) are created through such a ‘proactive’ agential dynamic? For the trainer, the seeming impossibility of stopping preemptive actions means that the focus of ‘proactive’ security-related actions is not on always preventing threats but on their mitigation and continued management. ‘Operational stuff needs to be structured as much as possible. This is what I mean by proactive’, the trainer further explains, highlighting the need for detailed, formalized plans for safe travel, for movement from home to office; for how to download suspicious documents form the Internet; and for how to behave online if targeted surveillance is suspected. Structure and formality are seen to bring efficiency to crisis response; to meet the challenge of a lack of time and space in the moment of preemptive violence.

This trainer’s approach is exemplary of a broader movement of ‘proactive’ action against digital security incidents within an increasingly formalized and specialized field. As of the writing of this chapter, an increasing number of transnational NGOs run hotlines, help desks, triage services, and information sharing platforms which document security incidents and mitigate their effects, encouraging human rights defenders and movement actors to reach out in event of crisis. Security specialists look for patterns in the nature and frequency of incidents, using this data to inform resource allocation and to secure infrastructures amidst anticipated disruption (Kazansky, forthcoming). The emphasis on structure, data, and continued vigilance result in a focus on resilience. A security specialist building out an information sharing platform argued that for her field, digital security has become about resilience ‘because shit is inevitably going to go wrong, and we want to enable our

partners to be resilient to the impact of that when they do happen' (Interview #42).

The proactive security stance, as embodied through the paradigm of data-driven resilience, hinges on two assumptions: first, that future harm will occur, but, second, the harm can be mitigated by collecting and synthesizing data about these harms and future potential threats on a continuous basis. As with the turn from 'reactive' to 'proactive' policing, per McCue (2015), resilience, as imagined within the digital security practices of these transnational civil society actors, constitutes a 'shift from describing the past' (24) to an approach focused on continued, data-driven management of anticipated harm. Effectively, individuals and groups affected by surveillance and digital threats are required to continuously anticipate preemption, a mind-twisting and circular proposition. It should be noted that resilience is a highly contested term endemic to the language of security regimes, state institutions, and corporations (Bourbeau, 2018; Coaffee, 2013; O'Malley; 2010). Resilience is critiqued by critical scholars of criminology and security as a regime of care premised on managerial logics of individual responsibility, propelled by state actors who have reneged on their duties of care towards citizens. This is one conception of resilience. On the other hand, however, resilience implies survival. Discussing findings from research and community organizing around data justice in three US cities, Petty et al., of the Our Data Bodies Project (2018) underline that people facing continued insecurity – here 'Charlotteans, Detroiters, and Angelinos' – are 'resilient in spite of persistent and destructive forms of surveillance and profiling'(1). As such, resilience here is understood as a necessity amidst longer-term struggles for social change; necessary because bringing an end to unacceptable practices and institutions takes time. Nonetheless, it is

one thing for a community to celebrate its own resilience and another thing for a violently negligent institution necessitate this resilience in the first place. In light of the ambivalence around the necessities and injustices of resilience, the question becomes how to attend to matters of every-day survival amidst probable future threats (in other words, to be resilient) while also moving towards a larger horizon of possible futures in which threats are not inevitable. This question is explored in the next case of the chapter.

## The proactivity of *dismantling of harmful systems through abolitionist refusal*

The last case discussed tactics to counter preemptive logics in the context of office raids. I documented the efforts made by NGOs and human rights defenders to 'proactively' ready themselves for future raids on their organizations, and how this kind of tactical safety work is conducive to a strategic focus on 'resilience' in the face of probable future threats. In this section of the chapter, I turn to another field work context where preemptive logics were countered, coming back to the work of the StopLAPD Spying Collation (SLSC) introduced at the start of the chapter. The SLSC is a group of volunteers that proactively challenge the preemptive logics exerted by a police force against populations living in the city of Los Angeles. While the security training in the first case was concerned with how to take tactical action against a particular preemptive manoeuvrer, the SLSC's focus is on challenging preemptive logics – and their carceral underpinnings – at an 'ecological' level (StopLAPD Spying and Free Radicals, 2020). Rather than conceding

to the inevitability of future threats and harms, the SLSC actively fights against their aura of inevitability through a focus on the abolition of the implicated systems and the re-imagining of just ones in their place. The vignette below introduces their work through an encounter at an international conference on digital rights and digital security. It then highlights how 'proactivity' is key to SLSC's fight against preemptive injustices, while also surfacing tensions between the different ways that transnational digital security specialists and grassroots community organisers contest surveillance and data related injustices.

In 2019, volunteer members of the SLSC traveled to Europe to give a presentation at an annual conference on Internet freedom and digital rights. In their presentation, they expounded an urgent case for why an abolitionist approach is necessary in order for movements to successfully tackle technologically related injustices, showcasing their work to dismantle predictive policing programmes in Los Angeles. The audience was largely comprised of nonprofit workers, tech activists, and digital security trainers from around the world. What united many of the audience members was their investment into the promotion of Internet freedom tools and digital security countermeasures such as encrypted email clients, VPNs and secure messaging applications. Making introductions at the front of the room, one SLSC volunteer began their presentation with a provocation: predictive policing, they said, 'isn't something we are going to solve with an encryption training' (field notes, 2019). With this statement, SLSC aimed to disrupt the audience's focus on technical mitigations for surveillance harms and data injustices. The presentation introduced the coalition's working principles and research, including their abolitionist analysis of the 'architecture of surveillance'(SLSC, 2015) and the 'ecological' configurations of

unjust algorithmic systems and their intwining with institutional racism (StopLAPD Spying and Free Radicals, 2020).

Throughout the presentation, the coalition emphasized the systemic nature of harm; arguing that the harms are not accidental but intentional, and that they did not just take place in 'a moment in time', but throughout a long history of injustice (field notes, 2019). Nor is the problem of predictive policing simply a matter of an unruly algorithm or 'dirty data' that can be fixed through technical 'de-biasing', they argued. The coalition's philosophy and working principles were not self-evident to at least some members of the audience, as became clear in the question and answer period that came at the end of the presentation. One member of the audience asked the coalition if they might consider training those affected by predictive policing harms in Los Angeles to use a secure computing system for their daily communications. A second asked: couldn't making policing more community-centric be a way forward? The SLSC provided the audience with emphatic answers for why these suggested actions are not a part of their repertoire. Regarding the suggestion to conduct digital security trainings on 'secure' tools, the SLCS reiterated that like any other group concerned with surveillance issues, everyday safety is a concern. However, the larger aim of their work is not to promote self-defensive digital security practice. In fact, the organization de-centres what they view as an unhelpful focus on technology and so-called tech-'fixes'. Rather, their work focuses on the dismantlement of the broader systems generative of surveillant and carceral logics and technologies. Coming back to the SLCS report introduced at the start of this chapter, the interviewed volunteer explained that:

> that's the biggest point of the phrase before the bullet hits the body. The focus is on structures. This isn't about

> just changing a programme or becoming more community oriented. The concern is not the bad apple. It's the system that is rotten at the core. It has to go completely (Interview #43).

The demand for the systemic dismantling of the racist, carceral 'stalker state' and its manifestations within 'smart' policing mechanisms is at the heart of SLCS's abolitionist approach to community organizing and policy change. In their community outreach strategy and in the awareness sessions they facilitate they are is focused on 'realizing there are programs, systems, structures that can essentially be ended and can be dismantled' (Interview #43). SLCS's work is part of a growing movement of grassroots initiatives engaged in abolitionist work that connects the ongoing fight against racism and carceral systems with technological injustices emerging in an era of datafication and ubiquitous digital surveillance (c.f. Benjamin, 2019; Datafication and Community Activism workshop, 2019; Emmer et al,. 2020; Gargandaran, 2020; Miller, 2019; Milner, 2019; STOPLAPD Spying Coalition 2018; 2020; Wang, 2018). This movement includes organisations such as the Carceral Tech Resistance Network[26], Critical Resistance[27], and Data for Black Lives[28].

Having introduced the stakes of SLCS' fight against the inevitability of harm, this section of the chapter explores how the time-space before preemptive violence figures into the abolitionist approach exemplified in SLCS's work. How to characterize the temporal dimensions of abolition in relation to the 'not-yet'? One answer is

26 https://www.carceraltech/

27 http://criticalresistance.org

28 https://d4bl.org

that abolition is about friction and slowness, as per Sarah T. Hamid of the Carceral Tech Resistance Network, who writes of her abolitionist work on technology that unlike the 'frictionless innovation' pushed by Silicon valley culture, 'you have to live in the friction. You have to be slow' (Hamid, 2020). Following Hamid's conceptualization of abolition, to refuse or to call for the dismantlement of something would imply a stoppage or slowing down of action. Slowness is also proposed as a counter to preemptive actions by Andrejevic et al., (2020) who critique preemption as a manifestation of accelerationist logics under high capitalism. Yet, the SLSC volunteer who I spoke to makes clear that if abolition is about friction and slowness, it is also about urgent action, explaining that 'we use the abolitionist framework because we don't want to lose time. Because we are losing people' (Interview, #43). This is to say that the urgency for the work of SLSC to shift from 'reactive' to 'proactive' action – in other words, to urgently grab back time, space and possibility – resonates with the urgency of the digital security trainer and human rights defenders in the preparedness training featured in the prior vignette. Describing the move to a proactive orientation, the interviewed SLSC volunteer explained: 'we were always in response mode. Something happened; someone died'. Eventually the organization began:

> moving away from just reacting but acting before everything happens...staying ahead of the game, pacing ourselves and are not just on being on the receiving end. Stopping it before it leads to someone's death. I go back to talking about the things we need to do before we die, things before we are murdered by the state; things to do before we are incarcerated (Interview #43).

In light of the urgency with which SLSC works, I return here to the question and answer period of the conference discussion held at the digital rights and Internet freedom conference. Following the first question about digital security, another audience member earnestly asked if SLSC had found an opportunity to sit down in dialogue with the police force in order to help them understand the harms of their actions to the community and aid them in reforming how it conducts its activities. For the SLSC, the invocation of community stakeholder participation as a solution to carceral harm tracks with an over-emphasis within civil society on the notion that harmful technologies can always be 'reformed'. 'You can't reform something based on such shaky grounds', the SLSC volunteer underlined for the audience. 'Sometimes reform leads to complicity in atrocities', he further argued, especially since the harms perpetrated by the police were not an isolated mistake, but rather, 'the harm is the point'. In light of this intentional harm, the volunteer asked the audience back, 'why take a seat at the table' in discussion? (field notes, 2019). Indeed, the SLSC provides a direct affront to the idea that policing – even where reframed as community driven, participatory, or democratic – is redeemable as an institution (which Gangadharan, 2020 characterises as a form of organized, community-level refusal). Where reformist policing initiatives strive for incremental change through existing institutional arrangements and small regulatory fixes, 'we don't want to waste time on legislation that will just blunt the edge of a knife, because a blunt knife is more painful.' (Interview #43).

Towards the goal of abolition rather than reform, the SLSC has engaged in a number of actions, making public records requests to learn more about policing programs and filing a Public Records lawsuit when they proved unresponsive (SLSC, 2019a; SLSC,

2019b); providing testimonies of police violence and community harm at public sessions; running community education seminars and teach-ins to map and directly challenge claims made by the police in public debates held at Board of Los Angeles Police Commissioners (BOPC) meetings, among other activities. It was their vocal demands at these meetings (spurred on also by the research featured in the report 'Before the Bullet Hits the Body) that lead the BOPC to hold a public hearing on Operation LASER in 2018. This public hearing resulted in the audit of the Strategic Extraction and Restoration (LASER) Program, to which the SLSC responded with further critique (SLSC, 2019b).

Around the time of our interview in 2019, SLSC was celebrating the end of the LASER program, bringing with it the end of the chronic offender bulletin, a risk scoring system which had disproportionally targeted the Black community (Puente, 2019). The SLSC attributes its end to the multi-year campaign it waged against it. At the time of its announcement, however, the police chief emphasized a continued faith in data-driven strategies of policing (Baek and Mooney, 2020). Hence, another goal of SLSC was the dismantlement of one of the other main predictive policing programmes, PredPol, a 'hot spot' based predictive policing program which broke the city of Los Angeles into 500-by-500 square foot blocks. Following another year of organising, its discontinuation was announced on April 21 2020. In a chapter covering the LAPD's decision in the LA times, the decision was attributed by Chief of Police Moore to economic reasons; 'the cost projections of hundreds of thousands of dollars' (Miller, 2020) – though public push-back by groups such as the SLSC had clearly caused it to lose its lustre. Whatever the reason given, the chief reiterated a belief in 'the underlying principles behind Pred-Pol' as 'valid' and pointed to a newly revised strategy

that would take its place, which he called ‘data-informed community policing’. This newest iteration of intelligence-led policing only served to confirm SLCS’ distrust in the notion of ‘community participation’ in policing as a viable way forward towards rectifying injustices. Here,‘community’ had been weaponized within the evolution of predictive policing towards further policing programmes and injustices. Hence, despite the end of the above programs, SLSC has had to remain ‘proactive’; vigilant about the rebranding of predictive policing under new names, covers, and rationales. The volunteered SLSC interviewee acknowledged the continuation of the fight: ‘we are staying ahead of the game and are pacing ourselves and we are not just on the receiving end...all of this is still a work in progress’(Interview #43).

# Tensions between resilience and refusal?

Having considered the SLSC’s abolitionist work to counter preemptive logics, I find it important to ask how the resilience strategy exemplified in the first case, and the abolitionist refusal discussed in the second case, sit in relation to one another as respective approaches to countering the harms of preemption. First, I underline once more that these two approaches both involve the embracing of a notion of a future-oriented ‘proactivity’ in response to harm. Yet this proactive orientation is imbricated differently in the two counter-preemptive contexts discussed in this chapter. Though I do not place the two cases or the approaches which they discuss in direct comparison with one another, my concern is with a potential tension in how these two respective approaches prefigure the relationship of groups and individuals to desirable and undesirable

futures. I point to the fact that for the group of human rights defenders and the digital security trainer featured in the first case, their proactive orientation was bound to the assumption that preemptive threats will continue to materialize in the future. The programme of resilience promoted by digital security actors in this case proffered a way to 'live' with or manage these continued, inevitable threats – but did not necessarily concern itself with a vision for how to tear out the roots of its source. Instead, resilience was elevated from a necessary, every-day tactic of survival to an overarching strategy and programme for data-driven action amidst assumed future threats. In contrast, the SLSC's work is explicitly orientated towards bringing an end to the source of the threat by dismantling the threatening ecology of technologies, institutions, and actors. Their abolitionist approach implies another orientation towards the future and its possibilities – one that is prefigured around a radical re-imagining of existing institutions and practices.

I underline that despite this tension arising around futurity and inevitability, the approaches taken in this chapter's two cases to counter preemption are certainly not mutually exclusive. Indeed, within the tactical dimensions of daily practice, efficient, structured security protocols may be applied towards the end goals of both resilience and abolition. Further, every-day resilience tactics are inherent to community centred work to counter the harms of data, per Petty et al., (2018) and Lewis et al., (2018: 38). Furthermore, as the participants of a community-centred workshop on activism taking place at UC Irvine (Datafication and Community Activism Workshop, 2019) underline, abolition work can – and should – allow for divergence and multiplicity in strategy, and do not necessarily imply the rejection of technological practices altogether. For example, Milner (2019) highlights that abolitionist work involves

making use of data and data-driven techniques towards anti-racist goals, a goal pursued by her organization Data for Black Lives. This confirms that, as I have also argued elsewhere (Kazansky, 2021; Kazansky and Milan, 2021) resisting surveillance and its harms often involves both co-opting and re-configuring its logics through the creative intwining of tools, tactics, and strategies from disparate realms. Hence, I argue that the tension in how resilience and refusal prefigure the future can be understood as part and parcel with the ambiguity that accompanies living with surveillance and injustice while also fighting for its end. Yet the potential for resilience strategies to reify resignation to inevitable future harm leads me to ask if there are there instances where the managerial, resilience-driven approaches to security arising in the context of transnational NGOs and security specialists might be more closely aligned with the abolition-centred work of grassroots community organizers. To ask this question more normatively, are there ethico-political considerations particular to civil society digital security practice which might suggest that resilience should be de-emphasized as the overarching strategy guiding this work? This I leave as a critical question for further future discussion.

# Between resilience and refusal: concluding thoughts

In this chapter, I have shown that for communities affected by preemptive and data-driven policing measures, acting on the space-time of the ‘before’ or ‘not-yet’ implies finding ways to interrupt the

ability for a small group of powerful actors to determine who deserves to live. But how? Drawing on the prevalently expressed need amongst people interviewed in my study to 'act proactively' in pursuit of safety in situations where preemptive threats loom over their work, I argue that proactivity can be understood as a precondition for counter-acting the preemptive, surveillant logics of violent state actors. Through the study of two cases of resistance to preemption, the chapter has shown that for communities affected by surveillance, to proactively act on the time before preemptive measures are enacted can imply a number of different paths of action. The chapter explored 'proactivity's as it arose within two contextual strategies of counter-preemption. The first case looked at how an imperative to act proactively arose in the context of digital security preparedness. I showed that for digital security actors striving for efficiency of digital security in response to emergencies, the proactive orientation involved creating structured protocols for behaviour in dangerous circumstances, and has lead security specialists to embrace the use of data to more efficiently anticipate and recover from future threats. I showed how this proactive orientation towards the future culminated in a programme of data-driven resilience focused on the management and mitigation of assumed future harm.

Second, I explored abolitionist refusal as a strategy of proactive counter-action, looking at how abolitionist community organizing has contributed to bringing an end to the preemptive threats of carceral, data-driven systems of surveillance, in the particular context of predictive policing in Los Angeles and the work of STOPLAPD Spying. I looked at how STOPLAPD Spying challenged the inevitability of future surveillance and related threats through a refusal to take a seat at the table with harmful actors and by refuting

the idea that reform can be achieved within an unjust system. In the end, I argue that the proactive orientation towards future harm, as discussed by interviewees and imbricated in their work to counter preemption, exemplifies the many ambiguities which accompany efforts to resist the hegemonic, 'anticipatory regimes' of contemporary surveillance (c.f. Amoore, 2013; Andrejevic et al. 2019 Mackenzie, 2013). While the ability by people put in harm's way to act proactively is exemplary of their agency and counter-power; the fact that they must do so highlights the extent of injustice that different groups and communities face. One could say that in the same way that resilience arises by necessity – so does proactivity, and in the same way that resilience is weaponized by institutions reneging on their duties of care, so does proactivity arise in the absence of protection from above. As such, I argue that those who study activism and movements should take care not to reify 'proactive' forms of action as an unproblematically positive phenomena in a datafied society, but to contextualize it instead as necessity by virtue of violence and injustice. Having made this argument, it is my hope that this exploration of proactivity can contribute to the interdisciplinary imperative espoused by critical scholars of data and automated systems to demonstrate that harmful technologies and institutions do not stand uncontested; nor are surveillance and harm inevitable facts of social life in a datafied society.