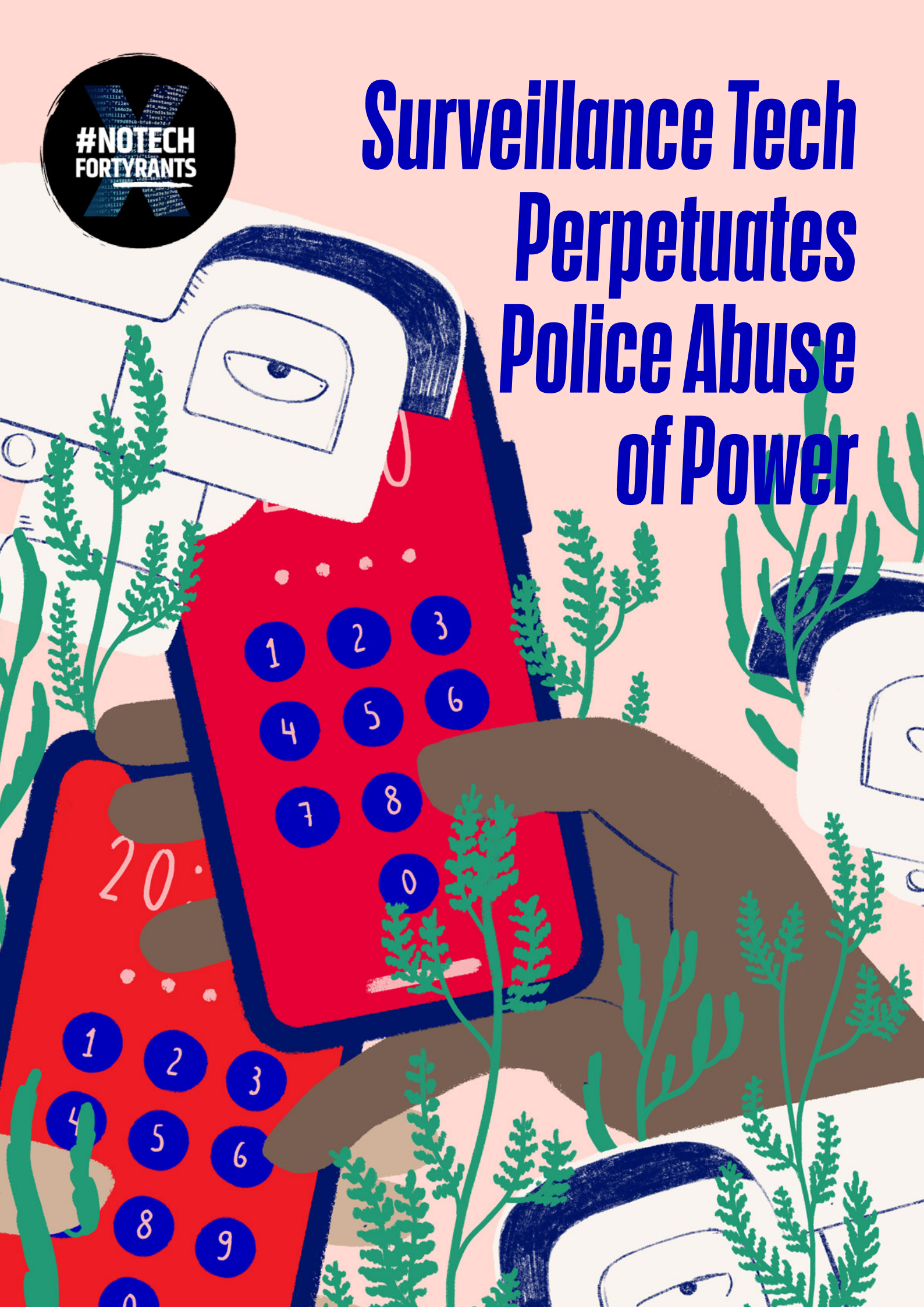
#NOTECH FORTYRANTS

Surveillance Tech Perpetuates Police Abuse of Power



EXECUTIVE SUMMARY

This report examines cases of police abuse of power in which surveillance technology plays a crucial role across various regional contexts. Too often, technology research focuses on criminalised individuals as perpetrators of abuse, implicitly framing law enforcement as problem-solvers rather than potential abusers on a systemic scale. Understanding policing powers through the lens of technology-augmented abuse helps us counter the use of digital technology against protestors and marginalised communities. We highlight how technology perpetuates and exacerbates police abuse, and we hope this work supports ongoing calls for justice.

Case Studies

We present the following seven case studies of tech-augmented police abuse of power:

LOCATION	CASE STUDY
UK	Abuse of law enforcement databases to perpetuate violence in intimate relationships
US	Smart street lights contained secret surveillance cameras
Brazil	Police video surveillance in the Jacarezinho favela
Mexico	Abuse of surveillance software to target activists, scientists, and journalists
UK	Abuse of surveillance footage for reality TV show
India	Police ask citizens to give them app access to cameras
Denmark	Use of technology to marginalise overpoliced communities

Key Dynamics of Tech-Facilitated Police Abuse

The case studies cumulatively show that police use of technology exacerbates abuse. This remains true in contexts where the technology use is clearly illegal, in cases where it has not been successfully legally challenged due to unevenly applied laws, and even in situations where this abuse remains lawful because the law protects and is in part shaped by police. Police have a well-documented history of abuse,[1] but the recent rise in adoption of advanced technologies has created a dangerous environment where police can assert control or authority on a much larger scale. We identify key underlying dynamics by which surveillance technology enhances police abuse of power:

THE MYTH OF PROTECTION THROUGH EFFICIENT SURVEILLANCE TECH: surveillance technologies are justified as a protection against threats such as terrorism or crime, building on the myth that more police equals more safety.

FOR PROFIT NOT PEOPLE: collaborations with the private sector which introduce a profit motive to data collection benefit the surveillance industry and not the public.

'FUNCTION CREEP': surveillance technology is used more broadly beyond its initially specified purpose.

INCENTIVISING DATA COLLECTION: the deployment of surveillance leads to increasing amounts of data being collected, often without a clear purpose.

EMBEDDING POWER AND MARGINALISATION: policing with surveillance technology reinscribes existing relationships of abuse and power between police and people.

SECRECY AND OBFUSCATION: surveillance technologies are often introduced in secret, and their use is often obfuscated.

LACK OF ACCOUNTABILITY: police abuse of surveillance technology is consistently difficult to bring to justice.

LAWS ARE NOT ENOUGH: laws and legal institutions do not adequately protect against police abuse of power through surveillance technologies.

RESISTANCE is forming through documentation, legal actions and challenging the underlying structures of police powers and the surveillance industry.

---

1. Vitale, Alex S. *The End of Policing*. NY: Verso Books, 2017; Cradle Community. *Brick by Brick: How We Build a World without Prisons*. Maidstone: Hajar Press, 2021.

Calls to Action

We call on fellow researchers, technologists, and civil society groups to divest from surveillance technology and policing:

RESEARCHERS: Stop recommending intrusive surveillance and repressive policing as solutions to social problems. Aim instead for research towards a generative, abolitionist project for a world where surveillance technology isn't necessary.

TECHNOLOGISTS: Avoid developing technology which expands police powers. Refuse the development of surveillance technology, embedding an abolitionist approach in your practice. Whenever possible, consider function creep and other long-term impacts of technologies whenever they are developed.

CIVIL SOCIETY: Campaign for greater democratic oversight and community accountability measures on police purchase and use of surveillance technology, in line with the aim of reducing police power.

DONATE OR JOIN US AT NO TECH FOR TYRANTS!
https://notechfortyrants.org/

Key Terms

ABUSE OF POWER: conventionally defined as an unlawful act committed by someone in a position of authority. In this report, we point to a variety of both lawful and unlawful acts committed by police officers that are nonetheless harmful as cases of abuse of power.

SURVEILLANCE: monitoring of behaviour or information for the purpose of information gathering, influencing, managing, or directing.

CARCERAL STATE: encompasses the formal institutions of the criminal justice system as well as the logics, ideologies, practices, and structures, that invest in punitive orientations to difference, to poverty, to struggles to social justice, and to the crossers of constructed borders of all kinds.[2]

FUNCTION CREEP: a process in which technology or information is used for a purpose that is not the original specified purpose.[3]

---

2. Adapted from Professor Ruby Tapia's definition, available on: French, Gabrielle, Allie Goodman, and Chloe Carlson. 'What Is the Carceral State?' *Documenting Criminalization and Confinement* (blog), 2 April 2021. https://storymaps.arcgis.com/stories/7ab5f5c3fbca46c38f0b2496bcaa5ab0.

3. Kornweitz, Arif. 'A New AI Lexicon: Function Creep'. *A New AI Lexicon*, 4 August 2021. https://medium.com/a-new-ai-lexicon/a-new-ai-lexicon-function-creep-1c20834fab4a.

TABLE OF CONTENTS

1 Introduction

We are told stories of "good guys" using surveillance technologies to catch "bad guys" (think of Batman behind a wall of blue screens). When we invest public resources in purchasing expensive surveillance devices for police forces, we might not imagine the police using them to monitor protesters, stalk their spouses, or sell footage to reality TV shows. In this report, we document these abuses, as well as a more pervasive and underlying form of abuse: surveilling communities which are already marginalised on the basis of race, gender, and class in a way which exposes them to entrenched police violence.

This report examines cases of police abuse of power in which surveillance technology plays a crucial role across various regional contexts. Uncovering cases of police abuse is crucial to supporting present calls for justice. Too often, technology research (both within industry and academia) focuses on criminalised individuals as perpetrators of abuse, implicitly framing law enforcement as problem-solvers rather than potential abusers. Understanding policing powers through the lens of technology-augmented abuse helps us counter impunity in the use of digital technology against protestors and marginalised communities.

We draw on existing abolitionist theories of policing, critical race theory critiques of surveillance technology, and feminist responses to technology-enabled coercive control. We then present seven case studies of police abuse of power in Western Europe, North America, South America, and South Asia.

These case studies (see table in Executive Summary above) cumulatively show that police use of technology becomes abusive and harmful in contexts where technology use is clearly illegal,[4] in cases where it has not been successfully legally

4. In this report, where we refer to a case as "illegal," we mean that based on public information available to us at the time of writing this report, we interpret one or multiple uses of technology in the context of the case to have violated a law. We are not making original claims about the legality of the actions of any actor named in this report, and note that others may interpret the events of the cases differently. The information in this report may not reflect legal proceedings that have taken place after the time of writing the report.

challenged due to unevenly applied laws, and even in situations where this abuse remains lawful because the law protects and is in part shaped by police. Police have a history of abuse but technology gives them more power to abuse at a larger scale.

We focus on technology because it can perpetuate and exacerbate abuse and can also be a point of intervention. In arguing that surveillance tech perpetuates police abuse of power we are not suggesting that technology is the source of all problems, but rather that it serves to exacerbate historically sedimented issues. The problem is not just about the technology and its design, but also about how technology is envisioned, deployed, and put to use by police agencies, as shown through this report. By campaigning for universities, companies, and governments to divest from surveillance technology, avoid developing technology which expands police powers, and stop recommending surveillance and law enforcement as a solution to social problems, we can reduce police powers and by extension the types of harms and abuse we identify in this report.

POSITIONALITY STATEMENT

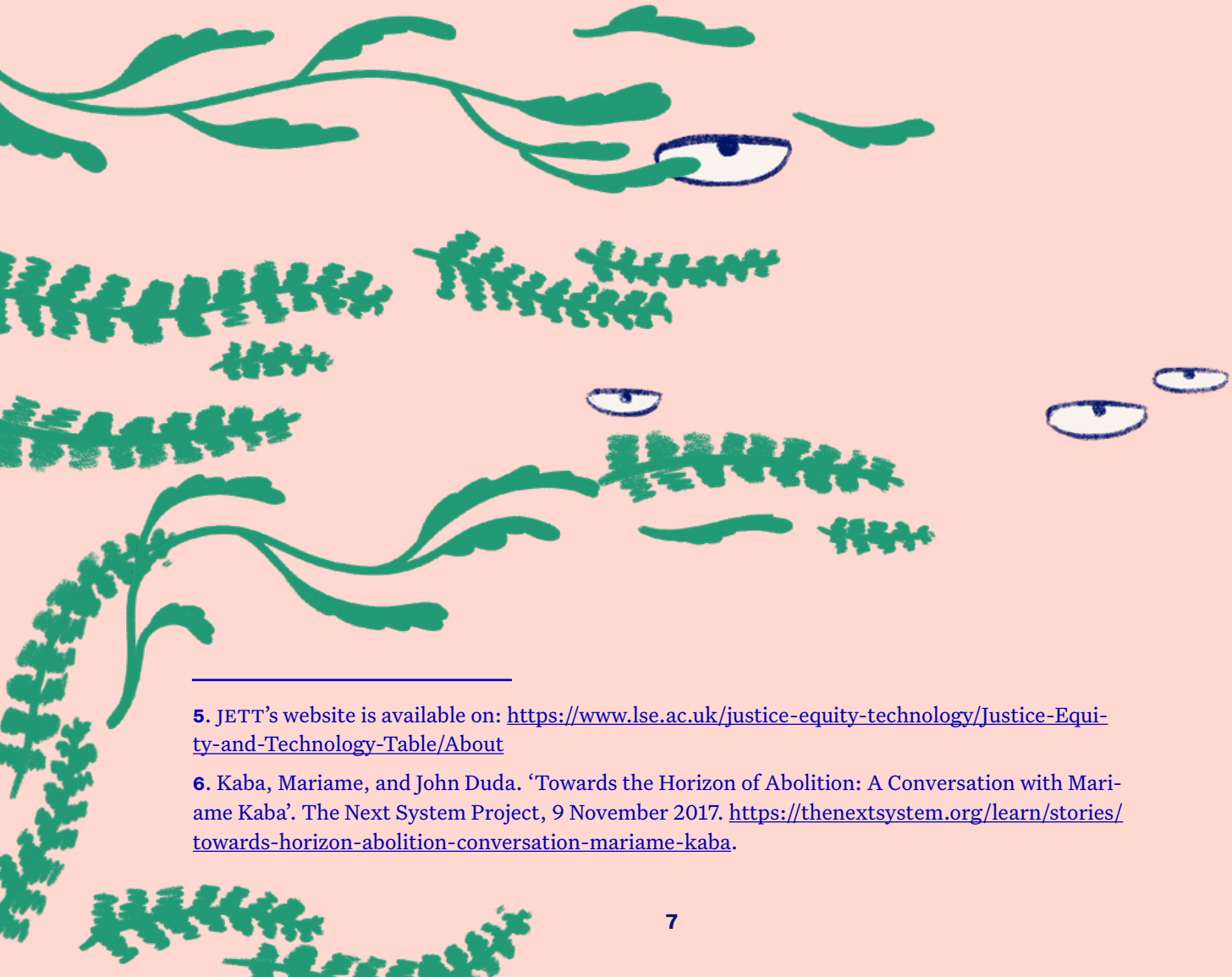
This report is written by members of No Tech For Tyrants (NT4T), a UK-based collective of volunteer organisers and researchers interested in dismantling the nexus between universities, technology, and border enforcement. Members of NT4T share commitments to anti-racism, as well as a desire to minimise the role of technology in perpetuating social and political oppression of marginalised communities.

We are mostly located within higher education institutions in the UK. Therefore we are all heavily influenced by Western education systems, which often perpetuate colonial approaches to scholarship. We come from various disciplinary backgrounds, including political philosophy, political theory, international relations, social science of the internet, criminology, techno-politics, computer science, critical race & digital studies, the black radical tradition, and political sociology. We identify variously and non-exhaustively as Brazilian, Greek-Lebanese, Polish, Mexican, American, South Asian, Hong Kong, middle-class, lesbian, queer, gay, man, woman, womxn, cisgendered, white, brown, and Neurodivergent. We are all in some way immigrants to the UK, which likely motivates our interest in border controls and surveillance. However, we also all have relatively secure immigration status and we were all unincarcerated at the time of research and writing. We all had the financial stability to contribute unpaid time to this project.

The working group met online regularly throughout the duration of this project, and the majority of the research and writing took place asynchronously: we assigned tasks and then added our work to shared documents for others to review and comment on. We continued this work in a low capacity environment, volunteering time alongside full-time jobs and studies. However, we were invigorated by the opportunity to do research together as a collective outside of the usual constraints of academia.

The report and preceding workshops (see Methods) were funded by a grant from the Justice and Equity Technology Table (JETT),[5] convened by researchers at the London School of Economics and Political Science. JETT is "a collaborative network-building effort to address the impacts of data-driven policing on racialised communities throughout Europe," of which No Tech For Tyrants is a member. JETT funded this research and convened a series of workshops with different research groups, but did not direct or limit the findings of this report.

Lastly, we are all working towards abolition. We all believe that police and prison systems are oppressive, and we aim to stop their expansion, defund, and ultimately abolish them in a gradual process that also includes building a world which does not need police or prisons (investing in well-resourced communities, preventative health, restorative justice, etc). While we share this common goal, we disagree in various ways (as is natural) about how this deconstruction should take place and what kind of society should replace our current system. However, we are inspired by writers such as Angela Davis, the Cradle Community Collective, Alex Vitale, and Sarah T. Hamid in our evolving understanding of how we get to "abolition as a horizon."[6]



5. JETT's website is available on: https://www.lse.ac.uk/justice-equity-technology/Justice-Equity-and-Technology-Table/About

6. Kaba, Mariame, and John Duda. 'Towards the Horizon of Abolition: A Conversation with Mariame Kaba'. The Next System Project, 9 November 2017. https://thenextsystem.org/learn/stories/towards-horizon-abolition-conversation-mariame-kaba.

We all believe that police and prison systems are oppressive, and we aim to stop their expansion, defund, and ultimately abolish them

2 Background and Literature Review

Our understanding of abuse of power draws on abolitionist, critical race, and feminist studies of gender-based violence. We briefly review each of these traditions in turn before answering the question "what is abuse?"

ABOLITIONIST THEORIES OF POLICING

As understanding the nexus among policing, technology, and abuse is the focus of this project, one of the crucial questions guiding our work relates to the nature of the relationship between policing and abuse of power. In characterising the relationship between police and abuse of power, one might locate abuse as the action of an *abusive individual*, and abusiveness as the property of an individual on the basis of their actions or dispositions. Following this line of thinking, police abuse of power occurs just when a police officer uses the power they have by virtue of being a police officer in a way that is harmful or wrong.

However, another approach to this question considers that policing is by definition an *abusive institution* in terms of its relationship to power. Individual acts and actors may vary in terms of degree of wrongness, harmfulness, and impropriety, however those parameters are defined; regardless of those variations, per this school of thought, *the use of power to carry out policing is fundamentally abusive*. Many scholars who engage this or similar approaches describe their work as *abolitionist* with relation to policing; they position their work as contributing to the normative project of abolishing the police (an end which is imagined in multiple configurations).

Police abolitionism is located within a broader tradition in scholarship and community organizing that focuses on the abolition of prisons and the Prison Industrial

Complex.[7] Much abolitionist scholarship is informed by, and seeks to contribute to, abolition-centred organizing and activism. As abolitionist scholars have noted, in the context of the United States, the advent of policing draws from the practice of policing Black slave communities and criminalizing Black people as part of a system of economic and political disenfranchisement.[8]

As scholar Ruha Benjamin writes, "calls for abolition are never simply about bringing harmful systems to an end but also about envisioning new ones. After all, the etymology of 'abolition' includes Latin root words for 'destroy' (*abolere*) and 'grow' (*olere*)." Abolitionist reforms divest resources from policing and reinvest in education, community health, affordable housing, and a broader support system.

While reformist reforms perpetuate or expand the scope of policing, abolitionist steps reduce the scope of policing and its harmful impacts.

For example, Tawana Petty writing as a part of the Our Data Bodies collective, argues for rejecting a "security mindset."[9] She notes security is primarily about securing items, property or identity rather than people: "Often, for undocumented, Black communities and other marginalised communities, the more secure a city proposes to be, the less safe those communities become. When cities invest in the security of neighbourhoods by adding surveillance cameras and increasing the militarization of police departments, it poses an imminent threat to those residents who are often deemed expendable. The security mindset without the human element is inherently unsafe." Petty argues safety is increased by nurturing relationships and providing adequate resources for health and mental health rather than building security systems.

Abolitionists make an important distinction between reformist and abolitionist steps in policing: While reformist reforms perpetuate or expand the scope of policing, abolitionist steps reduce the scope of policing and its harmful impacts. Common reformist suggestions include increasing police training and equipping officers with body cameras. These efforts are often touted for improving accountability, but

---

7. Davis, Angela Yvonne. *Are Prisons Obsolete?* New York: Seven Stories Press, 2003; Gilmore, Ruth Wilson. *Golden Gulag: Prisons, Surplus, Crisis, and Opposition in Globalizing California*. Berkeley: University of California Press, 2007; Kaba, Mariame, David Stein, and Dan Berger. "What Abolitionists Do," *Jacobin*, August 24, 2017. https://www.jacobinmag.com/2017/08/prison-abolition-reform-mass-incarceration.

8. Schenwar, Maya, Joe Macaré, Alana Yu-lan Price, and Alicia Garza, eds. *Who Do You Serve, Who Do You Protect?: Police Violence and Resistance in the United States*. Chicago: Haymarket Books, 2016.

9. Petty, Tawana. 'Safety vs. Security: Are You Safe or Are You Secure?' *Our Data Bodies* (blog), 18 January 2019. https://www.odbproject.org/2019/01/18/safety-vs-security-are-you-safe-or-are-you-secure/.

they rely on the assumption that policing "done right" increases safety. They also require funding and expand the scale of policing. In opposition, abolitionist steps such as withdrawing lethal policing tools reduce the capacity of police to exercise violence and increase budgets for community support.

The concept of "non-reformist reforms" can also be used to critique research framing: for example, framing algorithmic harms around "bias" suggests that more accurate data is the solution, at the risk of missing deeper questions about whether surveillance technologies should be used at all.[10]

CRITICAL RACE THEORY'S CRITIQUE OF SURVEILLANCE TECHNOLOGY

Under the veil of neutrality, law and technology are often considered to be solutions to police abuse of power. However, critical race theory (CRT) is an intellectual and social movement that interrogates the objectivity of these systems, arguing that racism is inherent in them. Drawing upon CRT, scholar Ruha Benjamin articulates that race is a social construct and racism also constructs, yielding social and economic value for some, while causing havoc on others.[11]

In the context of surveillance technologies, racism "is not only a symptom or outcome, but a precondition for the fabrication of such technologies."[12] In her book *Dark Matters*, Simone Browne explains that from 19th-century slave ships to post-9/11 airport security checkpoints, surveillance of blackness has been a norm, long before technology. She emphasizes that "rather than seeing surveillance as something inaugurated by new technologies...to see it as ongoing is to insist that we factor in how racism and antiblackness undergird and sustain the intersecting surveillances of our present order."[13] Surveillance technologies, especially used by the institution of policing, are inseparable from this long-existing order that extracts value from and abuses marginalised populations.

TECHNOLOGY-ENABLED COERCIVE CONTROL

Coercive control is a pattern of behaviour that is designed to assert influence and control over an individual's life using threats of harm, isolation, intimidation, and/or physical forms of violence, often resulting in a survivor losing a sense of their

---

10. Katell, Michael, Meg Young, Dharma Dailey, Bernease Herman, Vivian Guetler, Aaron Tam, Corinne Bintz, Daniella Raz, and P. M. Krafft. 'Toward Situated Interventions for Algorithmic Equity: Lessons from the Field'. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 45–55. Barcelona: ACM, 2020. https://doi.org/10.1145/3351095.3372874.

11. Benjamin, Ruha. *Race After Technology: Abolitionist Tools for the New Jim Code*. London: Polity, 2019.

12. Ibid.

13. Browne, Simone. *Dark Matters: On the Surveillance of Blackness*. Duke University Press, 2015, p. 8.

self-worth, bodily integrity, and safety.[14] Coercive control is increasingly used instead of "domestic violence" to encompass situations in which partners are not cohabitating, as well as to highlight that not all abuse includes physical violence. Technology-enabled coercive control refers to forms of coercive control which incorporate (usually digital) technology; in other words, the deliberate use of technologies or systems to scare, harass, coerce or stalk someone.

Literature on technology-enabled coercive control (or "tech abuse") points to the ways that technology can enhance abusers ability to exert control, for example through monitoring someone constantly using location-tracking, threatening to release embarrassing photos, or harassing through messages.[15] Uncovering these forms of abuse points to technology features—such as covert recording devices, spyware, or location-tracking—that is particularly likely to enable abusive behaviour. However, it is crucial to remember that forms of violence like coercive control are not new: the online forms of these abuses are continuations of older forms of oppression which uphold structures of dominance along the lines of gender, race, border policy, and heterosexism.

WHAT IS ABUSE?

We use perspectives from abolitionist, critical race, and feminist studies of gender-based violence to guide our understanding of police abuse. In particular, these frameworks moor our assertion that it is crucial to investigate police abuse of technology as, primarily, a form of abuse of power. Rather than approach police abuse of technology as a phenomenon unique or particular to the technologies in question, we ask: What role does technology play in larger patterns of abuse of power? What does this reveal to us about technology, power, and policing?

POLICE ABUSE IS INSTITUTIONAL. From abolitionist scholarship, we hear that abuse of power is inherent to policing as an institution, rather than particular to individual "bad apple" police officers—and equally, rather than individual technologies, regulatory frameworks, or laws about technology.

OPPRESSION IS NOT NEW. Critical race scholars show us that racism is a precondition—not an outcome—for surveillance technologies. Our understanding of technology, then, needs to take into account that new surveillance technologies cannot

---

14. Stark, Evan. *Coercive Control: The Entrapment of Women in Personal Life*. Interpersonal Violence. Oxford: Oxford University Press, 2007; Dana, Cuomo, and Natalie Dolci. 'Gender-Based Violence and Technology-Enabled Coercive Control in Seattle: Challenges & Opportunities'. TECC Whitepaper Series, 2019. https://sites.lafayette.edu/cuomod/files/2021/06/Technology-Enabled-Coercive-Control-Whitepaper-2019-1-1.pdf.

15. Freed, Diana, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. '"Is My Phone Hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence'. In *Proceedings of the ACM on Human-Computer Interaction*, 3:1–24, 2019. https://doi.org/10.1145/3359304.

and do not come into the world as "neutral." This would be the case even if we were to ignore the tendency for these technologies to serve the interests of those powerful enough to pay for the design and deployment of these technologies. We contend that police abuse of technology should not be approached, at least not by default, as something to be replaced simply by police "proper use" of technology. For example, where the technologies in question are built to surveil, extract from, and oppress racialised communities, such approaches would not mitigate or grapple with the root problem: racism. From feminist studies of technology-enabled coercive control, we further underscore this approach: abusive power relations are pre-existing. Certain technologies may facilitate abuse and control, but should not be understood as the origin.

ABUSE NEED NOT BE UNLAWFUL. Abuse of power is conventionally defined as an unlawful act committed by someone in a position of authority. In this report, we point to a variety of both lawful and unlawful acts committed by police officers that are nonetheless abusive, by which we mean unethical, harmful, and oppressive. We also draw on the notion of "coercive control" from the literature on gender-based violence and domestic violence. Although it is conventionally used only to describe abusive intimate relationships, it is also an apt description for the abusive dynamics that occur both when police officers are domestic abusers, and when they abuse police powers in relation to broader communities or marginalised groups.

Our understanding of power, then, is equally contested. We write with an understanding of power that is not specifically located in its definition as power "over" someone or something, or power as domination, but we do understand power in the context of policing to be domination and unjust power over others. Though this power is very influential, across the cases we highlight how people and organisations try to resist technology-facilitated police abuse.

This report does not start with a clear definition of abuse. Rather, we hope that through the case studies and exploration of situations that we deem abusive, we bring out a less-explored sense of *abuse* that does not follow clear lines of lawful versus unlawful action.

3 Methods

Our research question is: "How does surveillance technology enhance police abuse of power?" We chose a case study approach to understand the dynamics of police abuse of surveillance technology across various legal and geographical contexts. We selected cases on the basis of variations on the dimensions of theoretical interest, across two vectors: 1) the relationship between abuse and legality; and 2) the positioning across Global North and the Global South.[16] This allowed for cross-case comparison. We also chose case studies that were close to our local context in the UK, as well as in a variety of global contexts. In each case we selected, there was an element of inherent interest in the case or the circumstances surrounding it, for example because a researcher had a personal connection to or interest in the case.

While we do not necessarily aim to generalise, as each of the case studies are important in themselves, we do identify commonalities and differences among the cases. This allowed us to flesh out some key dynamics of how surveillance technology facilitates police abuse of power. Therefore our method falls into the category of "building block studies" which help to develop or test concepts and theories by identifying common patterns across cases.

We started by researching case studies and writing an initial draft of this report, after which we organised a workshop in which we brought together practitioners, researchers, and activists who work on themes that intersect with police abuse of technologies to share ideas, give feedback on a draft of this report, and discuss potential collaborations.

Following the workshop, we individually reviewed and reflected on the rich feedback that workshop participants shared with us. We then discussed these reflections together, taking note of feedback, challenges, and questions that stood out to multiple members of the group. This allowed us to determine where to focus our energy (please see **Workshop reflections**). We also presented versions of this project to audiences at the 2022 RightsCon and re:publica conferences.

16. Seawright, Jason, and John Gerring. "Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options." *Political Research Quarterly* (2014), doi:10.4135/9781473915480.n31.

WORKSHOP REFLECTIONS

In the interest of transparency, we present three takeaways from the workshop feedback and how we incorporated them in our work.

THEME 1: CASE SELECTION

During the workshop, participants had many questions and feedback related to our case selection. In particular, participants told us they could have used more clarity about how and why we chose the cases we did. Participants raised concerns that some of the higher-profile cases in the draft report did not represent the mundane, ongoing, everyday nature of police abuse of power.

For example, one of the cases we included in the draft report was about the Indian government requesting private information from technology companies (such as Zoom and Google) in order to use that information against climate activist Disha Ravi. In discussion, participants questioned the inclusion of this case (whose events were deemed egregious enough to receive international press coverage) over cases that might better demonstrate the role of technology companies in police abuse of power in India. In particular, participants noted that the case (and/or our write-up of it) did not engage with the caste-based nature of policing in India.

As a team, we agreed this was an important issue for us to consider: could we do better in choosing cases that demonstrate the structural, ongoing nature of technology-driven police abuses of power? In discussion after the workshop, we clarified our research question: we are not asking *whether* technology-facilitated police abuse of power happens, rather we are asking *how* it happens. We aim to continue to challenge our own notions of the "exceptional" and the "mundane" in relation to policing and technology.

We also came up with next steps about specific case studies in our report. Group members voted to replace the Disha Ravi case and replaced it with an alternative (Bhopal Eye) suggested by our participants. Based on the workshop discussions, we also added more detail to our case about policing in Denmark, and added a case from Brazil that focuses on "mundane" technology-enabled police abuse of power.

THEME 2: CONTEXT OF HISTORICAL ABUSE OF POWER & RESISTANCE

Participants from the Global South raised concerns about the lack of acknowledgement to local historical context and power dynamics in our cases. For example, Mexico's case in our report was about the use of the surveillance software Pegasus by law enforcement bodies. During the workshop discussion, our participant from Mexico called attention to the importance of understanding the role of these types of technologies as not recent, but rather a new version of surveillance and oppression tactics used before.

The workshop made it clear to us that we needed to do a better job at providing context for each case, such as historical context about policing and power in the society where the case takes place; and context about the everyday role of technology in policing. Participants also raised that resistance to policing and surveillance is a crucial part of what we consider relevant historical context, and noted that our report draft sometimes described abuse without acknowledging how people resist it.

In short, participants reminded us that the cases we chose did not take place in a vacuum: in order to substantively explore how police abuse power using technology in this case, we would need to ground our discussion in the history of policing, structural power, and technology in the local context.

Following this feedback, we revised each case study in the report to provide a clearer sense of its context. We drafted two questions to ask ourselves when adding in this context, to help ourselves think through each case critically:

- How do historical power dynamics manifest in policing in this case?
- What, if any, forms of resistance have emerged against this use of technology in policing? Can we link in collaborators and their work?

For example, in a case that discusses police officers in the UK using databases to commit domestic violence, we tied the case back to the ongoing patterns of gendered surveillance and abuse committed by British police, and how the public has protested these patterns, highlighting recent examples of organised resistance to gendered surveillance.

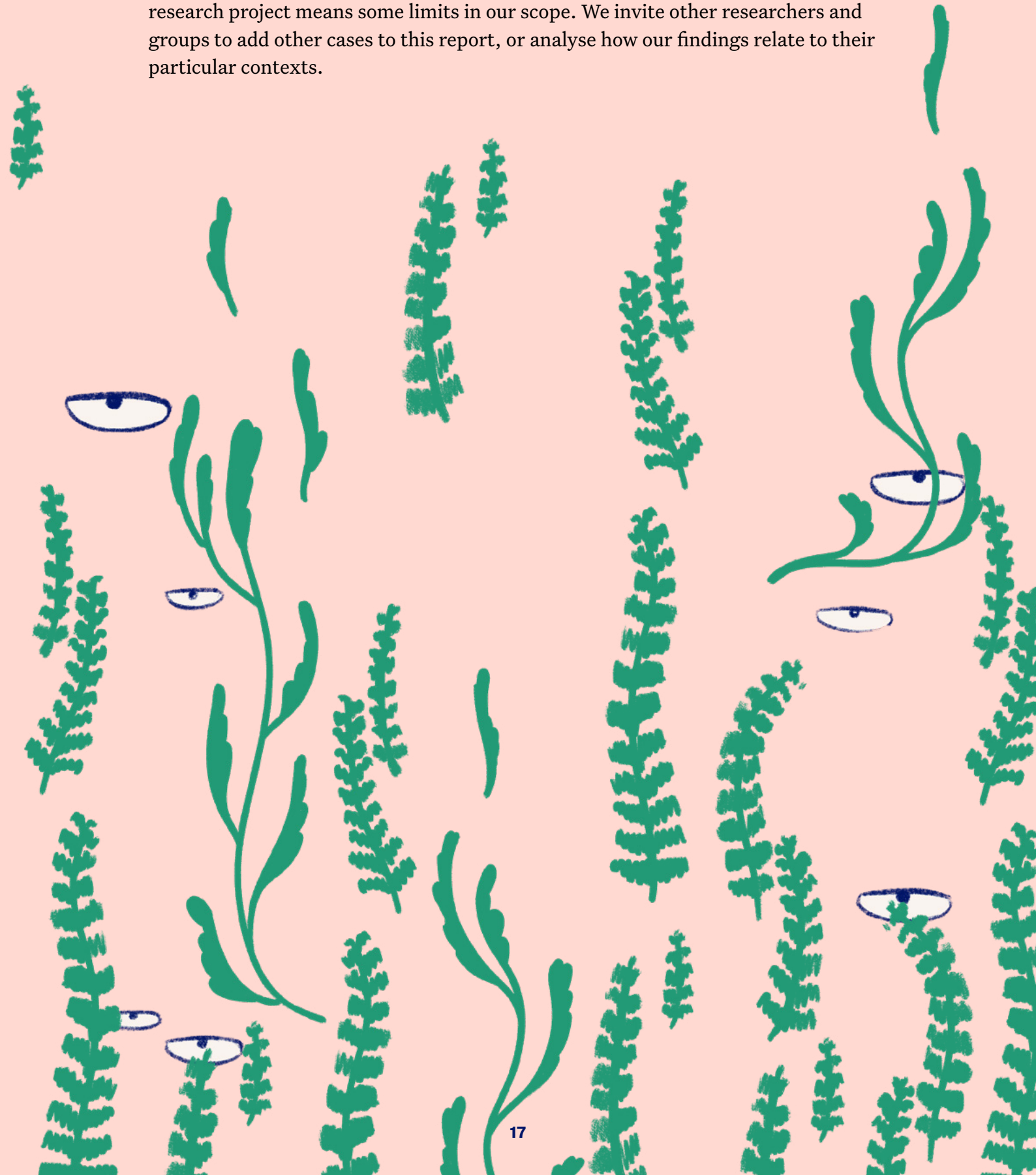
THEME 3: QUESTIONS AROUND ABOLITION

Lastly, an issue that emerged from the workshop was how we considered the role of policing in society more broadly. As we wrote the report, we had been framing the discussion around how surveillance technology enables police abuse. However, as workshop participants pointed out, the notion of "abuse" stops short of questioning the role of policing itself. The participants suggested thinking about what an abolitionist framework could mean for the report, particularly one that centres notions of "security, safety, belonging." Participants noted that, while it is important to emphasise the harmful and abusive impact of high tech policing, there could also be room to inject an affirmative perspective in our report.

This made us discuss more about how we position ourselves regarding police reform and abolition, as well as how our report can support this debate. We also wrote a positionality statement where we reflect on how our personal conditions inform our analysis in the report, including on the issue of abolition.

As we revised the report, we made time to discuss our understandings of transitional justice, abolition, and harm in relation to policing. This included going through our report together and discussing how each section aligns with our understanding of policing as an abusive institution, as opposed to one where abuses merely occur, and asking ourselves how our conclusions support the ongoing work towards a world without police.

We note some limitations in this report. Given that personal interest and connection was a factor in case selection, we recognize that a different group might have found different cases more salient. We do not claim to generalise universally on the basis of these cases; the dynamics that we identify are relevant to the cases we discuss, and may or may not be relevant to others. We drew primarily on English language news reports and resources, which may mean we missed the particularities of local contexts and languages. Finally, the limited budget and capacity of this research project means some limits in our scope. We invite other researchers and groups to add other cases to this report, or analyse how our findings relate to their particular contexts.



4 Case Studies

The following case studies cover a range of police abuse cases across different technologies, locations and legal systems. For each study, we documented the facts of the case, such as timescale, location, and who was involved. We paid particular attention to who was harmed in each case, as well as the legal situation, i.e. whether the actions described were lawful or unlawful in the local countries' legal framework. Lastly, we tried to determine what precisely made this use of technology abusive in each case.

1. TECH ABUSE IN INTIMATE RELATIONSHIPS IN THE UK

WHERE / WHEN?	Ongoing
WHO WAS INVOLVED?	Police officers and their (ex)partners, family members, friends, police oversight mechanisms
WHO WAS HARMED?	(ex)partners, family members, friends

Police officers commit domestic and sexual violence at much higher rates than the general population.[17] At least 129 women have approached the Centre for Women's Justice (CWJ) since 2019 with claims of being raped, beaten, and coerced by their

17. Two studies in the US have found that at least 40% of police officers' families experience domestic violence, in contrast to 10% of families in the general population (these measure self-reported and spouse-reported abuse, rather than conviction or investigation rates). In contrast, police officers seem to be convicted of domestic violence at a much lower rate than the general populations: a Freedom of Information request filed by the Centre for Women's Justice in the UK showed there were 19 convictions for 493 reports against police officers, a rate of 3.9%, while the general population rate is 6.2%. However, this is based on FOI data which is very incomplete—the response to the CWJ report described below illustrates the problems of incomplete record keeping, which means at the moment we most likely do not know enough to determine whether domestic abuse conviction rates are different for police officers

police officer spouses and partners.[18] An investigation by the CWJ in the UK in 2020 showed how incredibly difficult it is to get any form of justice or accountability in these cases.[19] Police officers who are abusers are likely to know how to manipulate the system to avoid penalty and/or shift blame to the victim. Furthermore, when officers involved in investigations into domestic violence by their colleagues, they may protect them by covering it up. Although the CWJ report notes it is unlikely to find "smoking gun" evidence of cover-ups, circumstantial evidence raised in the investigation related to this complaint is, in our opinion, highly suspect. Abusers in the police force can also draw on knowledge of and access to police systems to perpetuate abuse: for example, the CWJ includes testimonies of survivors who

Abusers in the police force can also draw on knowledge of and access to police systems to perpetuate abuse.

experienced stalking from former partners who were police officers. In these cases, perpetrators working in the police force may have had access to databases like criminal records and driving licenses; in one case, a survivor noted that her ex partner "was aware of information about her Community Psychiatric Nurse which caused her to think he may have accessed her medical records." Police officers accused of domestic violence could also access records related to their own criminal cases, or seek assistance from colleagues to access those records, in order to gain an advantage in court cases and investigations, as existing systems do not prevent this from happening.

While the existence of databases such as, for example, driving licences or traffic violations, is not inherently abusive, the fact that police officers have easy access to these databases is part of the problem, as police officers can and do use this access

---

than the general public. References: *On the front lines: Police stress and family well-being.* Hearing before the Select Committee on Children, Youth, and Families House of Representatives: Congress First Session May 20 1991. Washington DC: US Government Printing Office: 32-48. https://files.eric.ed.gov/fulltext/ED338997.pdf; Neidig, Peter H., Harold E. Russell and Albert F. Seng. "Interspousal aggression in law enforcement families: A preliminary investigation." *Police Studies* 15, no. 1(1992): 30-38; National Center For Women and Policing. 'Police Family Violence Fact Sheet'. Accessed 19 July 2022. https://web.archive.org/web/20181130155618/http://womenandpolicing.com/violenceFS.asp; Burmon, Andrew. 'Police and Violence at Home: Cops Abuse Wives and Kids at Staggering Rates'. *Fatherly*, 2 June 2020. https://www.fatherly.com/news/police-brutality-and-domestic-violence.

18. 'More than 100 women accuse police officers of domestic abuse, alleging "boys club" culture' *Channel 4 News,* 18 May 2021. https://www.channel4.com/news/more-than-100-women-accuse-police-officers-of-domestic-abuse-alleging-boys-club-culture

19. 'Police Officers Allowed to Abuse with Impunity in the "Locker-Room" Culture of UK Forces, Super-Complaint Reveals.' *Centre for Women's Justice*, 9 March 2020. https://www.centreforwomensjustice.org.uk/news/2020/3/9/police-officers-allowed-to-abuse-with-impunity-in-the-locker-room-culture-of-uk-forces-super-complaint-reveals.

for abuses such as stalking of current, former, and future partners as well as family members. For example, a married police officer in Sussex, UK searched police computer systems for a woman with whom he was interested in pursuing a romantic relationship.[20]

Use of such databases for stalking intimate partners are violations of police procedure,[21], and in our opinion, likely to violate data protection law. However the lack of accountability and recourse to justice creates an environment where police officers are "allowed to abuse with impunity in the 'locker room' culture of UK forces".[22] In June 2022, two years after the supra-complaint described above was initially filed, the government published a response based on a joint investigation by both government and independent police conduct oversight organisations.[23] Although the supra-complaint was upheld, with the investigation confirming that police-perpetrated domestic abuse is "significantly harming the interests of the public," the response did not endorse CWJ's primary proposed solution: i.e. that such cases be investigated by an external police force, with disciplinary aspects overseen by the Independent Office for Police Conduct (IOPC), and that survivors should have a bespoke reporting route to the IOPC. Therefore the supra-complaint outcome rejects the need for wholesale systems change, offering solutions which do not address the underlying problem identified by the CWJ, namely that connection between colleagues in police forces undermine responses to police abuse.[24]

This clear inadequacy in governance systems for egregious violations within police forces sheds light on the dynamics of technology-facilitated police abuse on larger scales: these include abuse of special powers (such as access to police databases), a lack of transparency, and a lack of accountability leading to impunity.

Such abuses are also a continuation of a broader pattern of gendered surveillance and abuse in British policing. In the ongoing "Spycops" scandal, eight women

---

20. Fuller, Christian. 'Sussex Police officer's warning for searching database for woman' *The Argus,* 24 Febuary. https://www.theargus.co.uk/news/19949182.sussex-police-officers-warning-searching-database-woman/#comments-anchor

21. Ibid.

22. We note that this claim related primarily to general attitudes that meant that the police fail to take robust action when domestic abuse was reported, rather than access to technology specifically. However, given broader accountability problems we think it is likely that cases of technology abuse woild similarly fail to be reported or investigated. 'Police Officers Allowed to Abuse with Impunity in the "Locker-Room" Culture of UK Forces, Super-Complaint Reveals.' *Centre for Women's Justice*, 9 March 2020. https://www.centreforwomensjustice.org.uk/news/2020/3/9/police-officers-allowed-to-abuse-with-impunity-in-the-locker-room-culture-of-uk-forces-super-complaint-reveals.

23. 'Police perpetrated domestic abuse: Report on the Centre for Women's Justice Super-complaint', *Gov.uk,* 30 June 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1086988/police-perpetrated-domestic-abuse-report-cwj-super-complaint.pdf

24. 'CWJ briefing on police perpetrated domestic abuse super-complaint outcome,' *Centre for Women's Justice*, 30 June 2022. https://static1.squarespace.com/static/5aa98420f2e6b1ba0c874e42/t/62bd7e5995cee616daf3c243/1656585818657/CWJ+briefing+on+super-complaint+outcome.30.6.22.final2.pdf

environmental activists were deceived to partake in long-term relationships with undercover police officers. These women successfully sued the Metropolitan Police. In the court case, Kate Wilson, one of the women who had experienced this, said that undercover police officers who spied on political groups were permitted, or tacitly encouraged, to form sexual relationships with women in order to help gather information on campaigners.[25] These practices, which are usually undocumented, point to a broader culture of institutionalised sexism.[26]

Resistance to this institutionalised misogyny has taken many forms. The CWJ supra-complaint is one example of resistance within established systems of complaint: although this process was slow and so far has not led to the systems change that the CWJ called for, it resulted in other branching forms of resistance. For example, although the initial complaint was based on the experiences of 19 women, after its publication CWJ was approached by 165 women with similar concerns.[27] This illustrates how a formal complaint can validate other survivors in complaining as well.[28] In addition to the CWJ super-complaint, the UK has seen a large mobilisation around police perpetrated gendered violence in the aftermath of the murder of Sarah Everard.[29] Protestors from the group Sister's Uncut have carried banners reading "police are perpetrators," set off bright blue smoke flares and activated 1,000 rape alarms outside Charing Cross police station. Sister's Uncut, which advocate for police budgets to be cut and funding for domestic and sexual abuse services reinstated has called on the UK public to "withdraw consent from policing", in reference to the tradition of "policing by consent" in the UK. They maintain that "more police powers will lead to more police violence and a society without police would be much safer."[30]

---

25. Evans, Rob. 'Police spy's bosses knew activist was being duped into sexual relationship, court told,' *The Guardian*, April 20, 2021, https://www.theguardian.com/uk-news/2021/apr/20/police-spys-bosses-knew-activist-was-being-duped-into-sexual-relationship-court-told

26. 'The Kate Wilson Case—Exposing Institutional Sexism of Spycops'. *Campaign Opposing Police Surveillance*, 24 April 2021. http://campaignopposingpolicesurveillance.com/2021/04/24/kate-wilson-case-exposing-institutional-sexism-spycops/.

27. 'CWJ briefing on police perpetrated domestic abuse super-complaint outcome,' *Centre for Women's Juctice*, 30 June 2022 https://static1.squarespace.com/static/5aa98420f2e6b1ba0c874e42/t/62bd7e5995cee616daf3c243/1656585818657/CWJ+briefing+on+super-complaint+outcome.30.6.22.final2.pdf

28. Ahmed, Sara. *Complaint!*. Durham: Duke University Press, 2021.

29. 'Sarah Everard: Protesters Demand "Radical Change" to Met Police.' *BBC News*, 12 March 2022. https://www.bbc.com/news/uk-england-london-60720907.

30. 'Sisters Uncut: PHOTOS: Sisters Uncut Set off 1000 Rape Alarms Outside Charing Cross Police Station.' *Sisters Uncut*, 12 March 2022. https://www.sistersuncut.org/2022/03/12/release-sisters-uncut-set-off-1000-rape-alarms-outside-charing-cross-police-station/.

2. SAN DIEGO SMART STREET LIGHTS IN THE U.S.

WHERE / WHEN?	San Diego, CA, 2016-2021
WHO WAS INVOLVED?	Smart street lights company (GE Current—subsidiary of General Electric, then Ubicquia), San Diego police, community organisers (TRUST coalition), city council
WHO WAS HARMED?	San Diego residents

When smart streetlights were installed in San Diego, California in 2017, they were pitched as an environmentally friendly and forward thinking "smart city" innovation for measuring air quality, reducing energy use, and producing data for efficient city operations. The lights were not intended as law enforcement surveillance tools. Yet, at some point in 2019, community organisers realised that law enforcement was requesting access to camera footage from the streetlights.[31] Many residents of San Diego were not even aware that these street lights had cameras. The TRUST Coalition, a group of more than 30 organisations, was formed to call for public oversight of city surveillance technology purchases.

Until March 2019, the police did not have a formal policy around the use of streetlight data. The San Diego Police Department argued that they only accessed footage for "serious crimes" such as murders, sexual assaults, and kidnappings. However the list of times the data had been used also included vandalism, dumping, and surveillance of Black Lives Matter protesters.[32] Without oversight, the list of what counted as "serious crimes" continued to expand.

After persistent media coverage, protest and campaigning with the City Council, the mayor of San Diego issued a directive to stop police use of the streetlights and stop recording.[33] However, this proved to be much harder than many expected. Turning off the cameras would have also forced hundreds of streetlights to go dark, because the two rely on the same power supply.[34] Furthermore, when the city requested that Ubicquia[35] reduce the retention time of the data from five days to zero

31. Perry, Tekla S. 'Cops Tap Smart Streetlights Sparking Controversy and Legislation'. *IEEE Spectrum*, 8 August 2020. https://spectrum.ieee.org/cops-smart-street-lights.

32. 'After Protests, SDPD Turned to Streetlight Cameras.' *Voice of San Diego*, 30 June 2020. https://voiceofsandiego.org/2020/06/30/morning-report-after-protests-sdpd-turned-to-streetlight-cameras/

33. Marx, Jesse. 'San Diego Can't Actually Turn Its Smart Streetlights Off.' *Voice of San Diego*, 2 November 2020. https://voiceofsandiego.org/2020/11/02/san-diego-cant-actually-turn-its-smart-streetlights-off/

34. Ibid.

35. Ubicquia is the company that owns the underlying technology of the smart streetlights, after purchasing it from GE Current who initially installed it.

days, Ubiquia refused, saying they would only do so once the city paid them money owed for operations. As a part of the deal, the city had also contracted with GE Current that the cloud operator, rather than the city, own any algorithms derived from the data, leaving the company with a financial incentive to keep collecting data.

In November 2020, the San Diego City Council gave initial approval to two ordinances to govern city surveillance technology and to create a community-led privacy advisory board meant to oversee purchases of surveillance technology (but without veto power). However, as of March 2022, the city has continued to purchase surveillance technology (in this case, a social media analytics service that tracks residents for "police" and "political" purposes) without public inquiry into its purpose or propriety. Although the ordinances were approved unanimously one and a half years ago, they require a second city council vote to pass, and the community coalition is still waiting.[36]

This case study illustrates the function creep of many "smart city" projects—the surveillance capabilities of smart streetlights were never publicly discussed—as well as the undemocratic tendencies in secretive public-private partnerships which give private companies access to resident data and power over delivery of public services. Lack of transparency contributes to abuse of power and enables function creep.

3. POLICE VIDEO SURVEILLANCE IN THE JACAREZINHO FAVELA, BRAZIL

WHERE / WHEN?	Rio de Janeiro, Brazil, 2021
WHO WAS INVOLVED?	Police of Rio de Janeiro (Military and Civilian), also including partnership with companies such as telecom Oi
WHO WAS HARMED?	Inhabitants of Rio, particularly those of the Jacarezinho favela

The Police of Rio de Janeiro has been implementing several new video surveillance systems. Since 2019, they have redoubled their surveillance with the implementation of new facial recognition and automated licence plate reader systems. These have been deployed without discussions with the community, impact risk assessments, or any kind of rigorous oversight. Moreover, such technologies generate serious possibilities for abuse (including false negatives), and were implemented despite results of a pilot study indicating their inefficacy. These systems continue a trajectory of

36. Custodio-Tan, Candice, Seth Hall and Geneviéve Jones-Wright. 'Opinion: San Diegans deserve a new surveillance ordinance. Until then, we're all in the dark.' *The San Diego Union Tribune*, 2 March 2022. https://www.sandiegouniontribune.com/opinion/commentary/story/2022-03-02/san-diego-city-surveillance-technology-trust

overpolicing for marginalised communities. Here, we particularly discuss the ongoing implementation of new video surveillance cameras in the favela of Jacarezinho.

It is important to situate policing in Brazil within a long history of colonial and racist structures. From its foundation in the 16th century, the city of Rio de Janeiro became a pole for the traffic of enslaved people from Africa, as well as the export of gold and sugar cane. In the 18th century, Rio was transformed into the capital of Brazil by the Portuguese Royal Family, who later moved to the city in 1808. The influx of people coming from Portugal led to the eviction of poorer people from the city centre (São Cristóvão) to new areas. This process, initiated over two centuries ago, continued well into the early 20th century, when poorer people (most of whom were previously enslaved) were removed from the city to the *favelas* in the hills as part of "modernization" efforts.

In response to such massacre, the Rio Police have argued for the implementation of new policing technologies in the Jacarezinho favela, particularly video monitoring.

These historically entrenched social issues are intrinsically connected to the current issues the city faces in matters of safety and security, as well as the forms of policing that take hold across different areas. The policing in the favelas is starkly different from that in affluent neighbourhoods. A recent example of this is the Jacarezinho massacre in May 2021: an operation by the Rio Civil Police in the favela which led to the killing of 28 people, making it the most lethal in Rio's history. Though the Police has since maintained the legality of such operation, it has been repudiated and criticised by many institutions for its abusive character, including the United Nations and Human Rights Watch.

In response to such massacre, the Rio Police have argued for the implementation of new policing technologies in the Jacarezinho favela, particularly video monitoring. This meant an expansion of a facial recognition[37] policing project launched in 2019, in partnership with telecom company Oi (which has been previously fined for the illegal sale of user data).[38] The implementation of 22 cameras including some facial recognition and licence plate reading capabilities would, in the words of the police, "contain and avoid actions against the lives of state agents and other citizens."[39]

---

37. The facial recognition technology used in Rio is based on technology from the UK company FaceWatch.

38. Kawaguti, Luis. 'Câmera inteligente no RJ terá sistema da Oi, multada por violar privacidade'. *UOL*, 24 January 2019. https://noticias.uol.com.br/cotidiano/ultimas-noticias/2019/01/24/cameras-monitoramento-carnaval-rio.htm

39. Secretaria de Estado de Policia Militar. 'Estudo Técnico Preliminar Sistema de Videomonitoramento em Vias Públicas (Jacarezinho).' Accessed 19 July 2022. https://drive.google.com/file/d/190WFEcBcZdm5ORiGjNk_a6v0IZnJcGva/view

As pointed out by the research group O Panóptico, the video monitoring of Jacarezinho with new technologies is being implemented without community consultation; will lead to disproportionate expenditures; and, most importantly, will not be based on any meaningful previous study of the impact of such new surveillance capabilities.[40] Instead, such technologies continue the trend of overpolicing of poor, black, and marginalised communities of Rio's favelas, which have long been criminalised. Moreover, as the report by the Police itself indicates, a key goal of the deployment of the cameras is to "produce proofs that corroborate reality and strengthen the affirmation of police innocence in future judicial trials." This means that, although implemented under the guise of the protection of the community, such camera systems have as a key goal the shielding of police officers for investigations of abuse (such as that which took shape after the Jacarezinho massacre).

Video monitoring continues a longer trajectory of criminalising poor communities and protecting police abuse. The implementation of new capabilities, including facial recognition and automated licence plate readers, raise new forms of potential abuse than previous CCTV video monitoring. The Rio Police have not indicated how data will be handled or deleted. Though they mention data will be kept for "60 days," there is no indication whether the data will be shared with other private or public institutions, as well as under what conditions. Moreover, these technologies have also been shown to make many mistakes, with a very high number of false positives which led to the frisking of innocent people. Considering that in 2019, across the entire country, 90% of people arrested utilising facial recognition in Brazil were Black, it is easy to see the outsized consequences for particular racialised groups.[41]

The implementation of video monitoring technologies enables both old and new forms of abuse by the Rio Police. These new systems haven't had their legality challenged in courts, and are being implemented with wide governmental support. Beyond the work of researchers and journalists to investigate and expose these issues, a bill has just been presented by state representatives from Rio and other Brazilian states' to ban the use of facial recognition in public spaces, including by police.[42] As indicated by O Panóptico, resources put in such experiments in policing infrastructure would be much better spent in dialogue with the local communities, including by funding education and support to families that are struggling financially.[43]

---

40. Nunes, Pablo, Mariah Rafaela Silva, and Samuel R. de Oliveira. 'A Rio of Cameras with Selective Eyes: The Use of Facial Recognition by the Rio de Janeiro State Police'. Centro de Estudos de Segurança e Cidadania (CESeC). Accessed 8 August 2022. https://opanoptico.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b_english.pdf.

41. Nunes, Pablo. 'Levantamento Revela Que 90,5% Dos Presos Por Monitoramento Facial No Brasil São Negros'. *The Intercept Brasil*, 21 November 2019. https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/.

42. 'Legislators from All Regions of Brazil Present Bills to Ban Facial Recognition in Public Spaces'. *Coding Rights*, 24 June 2022. https://medium.com/codingrights/legislators-from-all-regions-of-brazil-present-bills-to-ban-facial-recognition-in-public-spaces-31d8da0d3822.

43. Nunes, Pablo, Mariah Rafaela Silva, and Samuel R. de Oliveira. 'A Rio of Cameras with Selective Eyes: The Use of Facial Recognition by the Rio de Janeiro State Police.' Centro de Estudos de

4. ABUSE OF SURVEILLANCE SOFTWARE TO TARGET CIVILIANS, ACTIVISTS, SCIENTISTS, AND JOURNALISTS IN MEXICO

WHERE / WHEN?	Mexico, 2016 - 2021
WHO WAS INVOLVED?	Mexican federal and state police agencies, Mexican private companies, Israeli cyber-intelligence and security company NSO Group
WHO WAS HARMED?	Mexican civilians including human rights activists and investigators, scientists, health campaigners and journalists

When the investigation by Amnesty International and Forbidden Stories came out in July 2021, uncovering that 50 governments around the world spied on more than 50,000 activists, journalists, and political dissidents, it was found that Mexico was the country with the most potential targets—more than 15,000 people were targeted by the surveillance program.[44]

This mass surveillance scheme was made possible partly through software designed by NSO Group, an Israeli cyber-intelligence and security company. The Israeli firm has stated that their software Pegasus is a licensed malware that they provide to governments to pursue terrorists, drug traffickers, and other criminals.[45] But according to the investigations, amongst the targeted individuals are a minor child, human rights lawyers, international investigators, legislators, scientists, health campaigners, anti-corruption groups, journalists, and civic media.[46]

With high rates of violence against journalists in the country, this abuse of surveillance technology contains methods of surveillance and persecution that the current Mexican government—to date—also exercises against those who defend human rights.[47] This case reveals the trend that has been intensifying around the

---

Segurança e Cidadania (CESeC). Accessed 8 August 2022. https://opanoptico.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b_english.pdf.

44. Forbidden Stories. 'About the Pegasus Project.' https://forbiddenstories.org/about-the-pegasus-project/

45. Sheridan, Mary Beth. 'Mexico makes first arrest in Pegasus spying scandal.' *The Washington Post*, 9 November 2021.

https://www.washingtonpost.com/world/2021/11/09/mexico-pegasus-nso/

46. Lakhani, Nina. 'Fifty People Linked to Mexico's President among Potential Targets of NSO Clients'. *The Guardian*, 19 July 2021. https://www.theguardian.com/news/2021/jul/19/fifty-people-close-mexico-president-amlo-among-potential-targets-nso-clients.

47. 'ARTICLE 19 llama a respetar y no estigmatizar la labor de defensa de derechos humanos que realiza.' *ARTICLE 19*, 11 October 2020. https://articulo19.org/article-19-llama-a-respetar-y-no-estigmatizar-la-labor-de-defensa-de-derechos-humanos-que-realiza/.

use of highly invasive technologies that have been abused by government institutions towards civil society, without safeguards to protect human rights against the use they give them.[48] It also shows how surveillance technologies are justified as a protection against threats such as terrorism or crime, building on the myth that more policing equals more safety.

Thus we ask: Can the use of surveillance technology yield any positive outcomes for our communities when these technologies are being built and used by governments and tech companies who have a history of human rights abuse? And to what extent can we trust those with access to that technology to employ and regulate such tools for our communities safety when historical power dynamics say otherwise?

Significantly, private companies, government and law enforcement in Mexico are deeply interconnected and closely allied.[49] This broader context highlights key elements of how power dynamics and struggles may operate within and across geographical contexts. Though law enforcement supposedly works to increase safety measures, the mixing of private sectors with policing in Mexico exists in a continuum of accumulation of power. This leaves civil society marginalised from any safeguard. We argue that while surveillance industry markets itself as providing governments with the means to investigate serious matters of crime and terrorism, their products have become a convenient tool for undermining public accountability.[50]

The government's response to the revelations have also been criticised by civil society. In particular, the law enforcement agency responsible for investigating the abuse of the Pegasus tool were themselves involved in its procurement, increasing the likelihood of institutional bias in the investigation.[51] While one arrest was made in November, 2021 of a businessman accused of unlawfully using the spyware, the government's own role and use of the scandal has not been interrogated, calling to attention the lack of institutional accountability for government misuse of surveillance technology. The revelations about widespread abuse of this surveillance tool have drawn international condemnation, including sanctions and lawsuits.[52] While the scandal has also exposed alarming regulatory gaps with regard to emerging

---

48. K., Alex. 'Lo que revela #PegasusProject en Mexico.' *Twitter*, 19 July 2021. https://twitter.com/KafSofit/status/1416882637549891584?s=20&t=D9K73OXcuR6Db9l3tyq5ig.

49. This is corroborated by a dozen contracts disseminated by the Network in Defense of Digital Rights, revealing how a network of private companies was in charge of acquiring the software and then marketing it to public entities. Reference: 'Lo que sabemos de las autoridades que adquirieron Pegasus en México.' *R3D*. 23 July 2021. https://r3d.mx/2021/07/23/autoridades-pegasus-mexico/

50. Deibert, Ron. 'Protecting society from surveillance spyware.' *Issues in Science and Technology*, 2022. https://issues.org/surveillance-spyware-uso-group-pegasus-citizen-lab/

51. Asher-Schapiro, Avi, and Christine Murray. 'INSIGHT-Pegasus Spyware Scandal: Years of Questions, No Answers for Mexico Victims'. *Reuters*, 9 August 2021. https://www.reuters.com/article/mexico-tech-surveillance-idUSL8N2PD6BQ

52. Robinson, Kali. 'How Israel's Pegasus Spyware Stoked the Surveillance Debate.' *Council on Foreign Relations*, 2022. https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate

surveillance technologies, we posit that regulations are not enough as historical power dynamics remain in place.

This broader context accentuates key elements of police abuse of power enhanced by surveillance technology: when the cyber surveillance market meets operations by law enforcement institutions that are already known to be corrupt and how police abuse of surveillance technology is consistently difficult to bring to justice. Questioning how the use of surveillance technology enhances abuse of police powers, which for most Mexicans was not shocking nor aberrant but a new version of tactics that have already been used before, and understanding how historical power dynamics work can give us knowledge for considering the many venues for resisting these technologies.

5. ABUSE OF SURVEILLANCE FOOTAGE FOR UK REALITY TV SHOW

WHERE / WHEN?	2000s-2016
WHO WAS INVOLVED?	Thames Valley Police, Road Wars reality TV show, Oxford residents
WHO WAS HARMED?	Residents of Oxford filmed in encounters with police

When the police collect surveillance footage, what is the footage used for? We are often made to assume that surveillance footage is a tool used by police for reducing "crime" in our communities (for example, CCTV) and for ensuring accountability (for example, dashcams and bodycams).

For a number of years in the 2000s, the Thames Valley Police based in the UK gave surveillance footage to the reality television show Road Wars, a reality television series that followed police officers.[53]

In using surveillance footage for episodes of Road Wars, the police used technology quoted to the public as a safety and accountability measure for the purposes of profit and entertainment, not to mention the public dissemination of a police-controlled narrative of the events transpiring in the footage. It appears that at the time, there was no legal injunction prohibiting the police from selling and using privileged surveillance footage for the purpose of reality television like Road Wars. Regardless of the legal situation, we consider this a case of abuse of power through the technology entrusted to the police.

We ask: To what extent does sharing this footage really serve to protect or defend or be accountable to our communities? Are the police making good use of sur-

53. 'Road Wars (TV Series).' *Wikipedia*, 11 February 2022. https://en.wikipedia.org/w/index.php?title=Road_Wars_(TV_series)&oldid=1071217263.

veillance footage by broadcasting the arrests of marginalised and racialised individuals with blurred faces, in a context that categorises them as primarily perpetrators and criminals? In some cases recorded individuals do not get a chance to consent to or be notified about footage of them that is shared on reality "copaganda"[54] shows. Is this the public accountability that police surveillance technology is marketed as providing? We see these questions as imperative to understanding the violent hierarchies of power and control at the heart of policing writ large, and underlying many of the deeply harmful technological practices undertaken by police forces.

When asked via Freedom of Information Act request to share further information about their stance on police reality television work and any active engagements with police reality television, the Thames Valley Police refused to answer, noting that doing so would exceed the resource limit for FOIA requests. When asked in the same request if they currently sold dashcam footage or made it available, the Thames Valley Police linked to an unavailable statement on their website.[55]

Above, we argue that the use of police surveillance footage for Road Wars is an abuse of power. This abuse did not take place in a vacuum: Road Wars is not the only television show that has used police camera footage, and certainly not the only television that has invited us to share the perspective of agents of the police. Shows use police footage or other forms of surveillance footage normalise surveillance and centre the perspective of the police as heros fighting "the bad guys" and "dumb criminals."[56] This broader context highlights a key element of police power: the power to shape and control the stories we consume about policing and criminality. Questioning the pro-police media we are given and supporting those who push back on the social power inequities reproduced in the entertainment industry are important steps towards reducing the power police have to abuse our communities.[57]

This broader context highlights a key element of police power: the power to shape and control the stories we consume about policing and criminality.

54. "Copaganda" is a term used to describe entertainment media that centres the perspective of police

55. 'Media Appearances of Law Enforcement Agencies—a Freedom of Information Request to Thames Valley Police.' *WhatDoTheyKnow*, 20 February 2021. https://www.whatdotheyknow.com/request/media_appearances_of_law_enforce_45.

56. Ongweso Jr, Edward. '"Ring Nation" Is Amazon's Reality Show for Our Surveillance Dystopia'. *Vice*, 11 August 2022. https://www.vice.com/en/article/7k8×49/ring-nation-is-amazons-reality-show-for-our-surveillance-dystopia.

57. Cradle Community. "Copaganda" in *Brick By Brick: How We Build a World Without Prisons*. Hajar Press, 2021: 95-99.

6. THE BHOPAL EYE APP IN INDIA

WHERE / WHEN?	Bhopal, Madhya Pradesh, India; November 2019-present
WHO WAS INVOLVED?	Bhopal police, residents of Bhopal, Citizen COP Foundation
WHO WAS HARMED?	Residents of Bhopal

In November 2019, the police in Bhopal, Madhya Pradesh, India announced the creation of 'Bhopal Eye,' an app that seeks to involve city residents in crime detection by securing online access to CCTV cameras in local businesses and outside people's homes.[58]

The app is meant for "people of the city [to] easily share the feed of their private cameras which can be accessed by the police administration. The police officials can go through the feed in a master control room and analyse how they can prevent and solve crimes."[59] The app allows the police to access live feeds from people's cameras. It also allows citizens to report so-called suspicious activities or individuals to the police. To do so, citizens need to share the precise geographical location of their camera, as well as port number, URL, and login details to access it remotely.

The Bhopal Eye app was developed in association with Citizen COP Foundation, a non-profit organisation that develops apps on which, among other functions, people can report suspected crime to their local police departments. Their self-described goal is building a "technological bridge between citizens and the police."[60] The app is marketed to the public as a means to assist the police in crime prevention efforts. Residents of Bhopal are told that "if you've been wanting to help the police administration in any way, especially to improve the security status of Bhopal, then download the application and start right away!"[61]

The implementation of Bhopal Eye illustrates the mundane abuse of power typical of policing. Outside of individual instances of people being harmed by the power that police are given license to exert, we see this case study as an example of how the police use technology to exert power over people—asking them to spy on their neighbours and expand police access to and influence over people's lives—to the detriment of communities already disproportionately targeted by policing.

---

58. 'Only 100 Registrations on Bhopal Eye App.' *The Free Press Journal,* 4 January 2020. https://www.freepressjournal.in/bhopal/only-100-registrations-on-bhopal-eye-app.

59. 'Bhopal Eye - Bhopal Police – Apps on Google Play.' *Google Play Store*. Accessed May 15, 2022. https://play.google.com/store/apps/details?id=com.info.bhopaleye&hl=en_GB&gl=US

60. The CitizenCop's website can be found on: https://www.citizencop.org/

61. 'Bhopal Eye - Bhopal Police (App Page)'. Accessed 25 July 2022. https://apppage.net/preview/com.info.bhopaleye.

The historical and social context in which this app operates is charged with discrimination, casteism and more generally oversurveillance of marginalised communities. This complex social context assumes several risks in the surveillance practices that are pushed onto citizens, especially in the context of the global pandemic. In a report on pandemic policing and sanctioned violence in Madhya Pradesh, the Criminal Justice and Police Accountability Project describes a systemic bias against the poor and marginalised communities such as Scheduled Castes (SC), Scheduled Tribes (ST), Other Backward Classes (OBCs), and religious minorities like Muslims.[62] The approach brings focus on what can be considered low level offences and blue collar, highlighting types of crime that are more easily captured and assessed by surveillance cameras in neighbourhoods.

The historical and social context in which this app operates is charged with discrimination, casteism and more generally oversurveillance of marginalised communities.

There are no laws explicitly regulating police use of surveillance technology of this nature in India. Although the Supreme Court of India reaffirmed the constitutional right to privacy in 2017, law enforcement (and government surveillance more broadly) is frequently exonerated in court, even in the rare cases where its legality is challenged.[63]

Bhopal is the second city in the country to have adopted this system after Surat. Similar trends of neighbourhood surveillance by police using people's privately installed outside cameras can be observed around the globe, for example in the case of Amazon Ring cameras used as an extension of police surveillance apparatus in American neighbourhoods.[64] In both geographical contexts it is well documented that law enforcement activities are disproportionately focused on surveillance and enforcement against already marginalised communities. It follows that we can reasonably expect the implementation of Bhopal Eye to exacerbate such discriminatory practices and police abuse of power.

At least one source notes low uptake of the app by local residents.[65] While this could be for a number of reasons, it leads us to ask: How could the resources used to

---

62. Ameya Bokil, Avaneendra Khare, Nikita Sonavane, Srujana Bej and Vaishali Janarthanan. 'Settled Habits, New Tricks: Casteist Policing Meets Big Tech in India.' *TNI Long Reads,* May 2021. https://longreads.tni.org/stateofpower/settled-habits-new-tricks-casteist-policing-meets-big-tech-in-india

63. Puttaswamy v. Union of India (II), (2019) 1 SCC 1; Mr. Virendra Khanna vs State Of Karnataka, [W.P. No. 11759/2020].

64. Bridges, Lauren. 'Infrastructural Obfuscation: Unpacking the Carceral Logics of the Ring Surveillant Assemblage'. *Information, Communication & Society* 24, no. 6 (26 April 2021): 830–49. https://doi.org/10.1080/1369118X.2021.1909097.

65. 'Only 100 Registrations on Bhopal Eye App.' *The Free Press Journal,* 4 January 2020. https://www.freepressjournal.in/bhopal/only-100-registrations-on-bhopal-eye-app.

develop the Bhopal Eye app perhaps have been used instead? Could they have built or invested in resources that local residents might find more useful than surveillance?

7. PALANTIR DEPLOYMENT IN DENMARK, PARTICULARLY IN THE CONTEXT OF RACIALISED COMMUNITIES

WHERE / WHEN?	Denmark, since 2015
WHO WAS INVOLVED?	Danish police, Palantir
WHO WAS HARMED?	People in Denmark, particularly marginalised and racialised communities

In 2017, the Danish Police drafted a legislation—led by its Data Protection Officer, and in collaboration with Palantir—that would exempt them from the European Commission's law enforcement data protection regulation.[66] Following the 2016 purchase of software from Palantir Technologies, in 2017 the Danish Ministry of Justice presented a draft legislation for public consultation that would allow the processing of personal data through the Palantir-supplied software. As of late 2018, the Danish police and Palantir enjoy a contractual relationship for the deployment of POL-INTEL and PET-INTEL, the former of which is based on Palantir Gotham.

POL-INTEL works as a system to integrate and search through previously siloed databases (e.g. vehicle registration, police cases, weapon permits). By making such information actionable, their argument goes, this would allow for more precise and intelligent data-based decisions. The platform thus allows for ready access to information about citizens, which can be used to investigate linkages, as well as to spot previously unknown connections. A key consequence of the purchase of Palantir software is an increased incentive to collect more data on all citizens, a situation which is even worse for those that have previously been in contact with the criminal justice system.[67] This data, once collected, can be used in ways that seriously impact marginalised people. For example, in 2017 both Germany and Denmark expanded laws that enabled immigration officials to extract data from asylum seeker's phones in order to establish evidence or justifications for deportation.[68]

66. Lund, Jesper. 'New legal framework for predictive policing in Denmark.' *EDRI*, 22 February 2017. https://edri.org/our-work/new-legal-framework-for-predictive-policing-in-denmark/

67. Brayne, Sarah. *Predict and Surveil: Data, Discretion, and the Future of Policing*. New York: Oxford University Press, 2021.

68. Meaker, Morgan. 'Europe Is Using Smartphone Data as a Weapon to Deport Refugees'. *Wired UK*, 2 July 2018. https://www.wired.co.uk/article/europe-immigration-refugees-smartphone-metadata-deportations.

One key use of analysing crime patterns in Palantir is to draw heat maps of recorded crimes in each area of the country.[69] This system, named SmartSpot, is now used to decide the location of police patrols. However, such systems can lead to overpolicing of areas where crime has previously occurred. Such "feedback loops"[70] serve to further entrench existing biases. Rather than predicting crime, they reproduce already existing unequal conditions, serving to further marginalise communities which are already overpoliced.

In particular, activists have sounded the alarm on the use of POL-INTEL on people living in "ghettoised" communities, which are targeted by the Danish government on a racialised basis. In 2010, Denmark started making a distinction between "Western" and "Non-Western" Danes.[71] In 2018, Denmark announced the controversially named "ghetto package", which sought to intervene in areas with more non-western Danes than western Danes, because "[Western] Danes should not be a minority in any housing area."[72] The ghetto package policies are enabled by massive databases such as the residence registrar, employment, taxation, education and criminal convictions. These databases provide the basis of a scoring system that classified neighbourhoods as ghettos on the basis of residents' income, employment status, education levels, number of criminal convictions, and "non-Western background."[73]

---

69. In the beginning, this technique of "forecasting" was construed as "predictive policing" by Danish Police, as shown in: Kulager, Frederik. 'Politiet har opdaget, at data kan spå. Nu kan de forudse forbrydelser'. Zetland, 19 December 2016. https://www.zetland.dk/historie/s81PmbGv-aOZ-j67pz-50e53; Kulager, Frederik. 'Vi prøvede dansk politis nye, kontroversielle datavåben. Det tog os ti minutter at opklare en sag om hashsmugling'. *Zetland*, 20 June 2018. https://www.zetland.dk/historie/sop1JZkz-aOZj67pz-e4a92; Kulager, Frederik. 'For fire år siden fik politiet et "supervåben". Her er, hvordan det har transformeret ordensmagten'. *Zetland*, 4 May 2021. https://www.zetland.dk/historie/sO9kBG7W-aOZj67pz-04ca0.

70. Lund, Jesper. 'Pitfalls and Possibilities with Intelligence-led Policing.' *ITU CUPP Seminar*, 14 December 2021. https://cuppresearch.info/fileadmin/user_upload/Pitfalls_and_Possibilities_with_ILP__ITPOL_-_Jesper_Lund_.pdf

71. O'Sullivan, Feargus. 'How Denmark's "Ghetto List" Is Ripping Apart Migrant Communities'. *The Guardian*, 11 March 2020. https://www.theguardian.com/world/2020/mar/11/how-denmarks-ghetto-list-is-ripping-apart-migrant-communities.

72. In 2021, Denmark moved away from the term "ghetto," while further proposing that "the share of residents of 'Non-Western' origin in each neighbourhood be limited to a maximum of 30% within 10 years." Source: Skifter Andersen, Hans. 'Denmark's Attack on 'Non-Western' Neighbourhoods.' EUROPP LSE Blog, 14 April 2021. https://blogs.lse.ac.uk/europpblog/2021/04/14/denmarks-attack-on-non-western-neighbourhoods/; Agence France-Presse. "Denmark Plans to Limit 'non-Western' Residents in Disadvantaged Areas." *The Guardian*, 17 March 2021. https://www.theguardian.com/world/2021/mar/17/denmark-plans-to-limit-non-western-residents-in-disadvantaged-areas

73. It is important to mention that only education recognised by Danish authorities counts now, a move that further discriminates against immigrants. It has been found that if education obtained abroad counted, 20 out of the 28 "ghetto" regions would not be considered such. Reference: Toft, Nana. '20 ud af 28 områder ville ryge af 'ghetto-listen', hvis ministeriet valgte at tælle alle beboernes uddannelser med.' *Fagbladet Boligen,* 23 November 2020. https://fagbladetboligen.dk/alle-nyheder/2020/november/20-ud-af-28-omrader-ville-ryge-af-ghetto-listen-hvis-ministeriet-valgte-at-taelle-alle-beboernes-uddannelser-med/

Therefore criminal justice databases can impact housing security not just for criminalised people, but also their family and neighbours. The punitive measures in the "ghetto package" include the provision that some crimes committed within those areas may receive double the punishment by courts. This means that policing data is used both as a way for determining future police patrol placement and for determining which areas of the city should be more punished, thus further criminalising racialised communities.

While initially proposed as a solution to terrorism,[74] Palantir's software is now used more broadly for policing around the world. In Denmark, the Palantir contract was designed to comply with the law, but nevertheless the use of these systems may often yield inaccurate and false results, usually on the premise of historical data already skewed towards certain ethnic designations based on pre-existing discriminatory practice (feedback loops).[75] Seen in a broader historical context, these policies represent the culmination of a process by which anti-immigration policies have gradually moved from being a fringe proposition by far-right parties to being adopted and actioned on by centrist parties.

There has been no mass society resistance to the use of Palantir's technology in policing, possibly due to the high trust among some citizens in the Danish state and the opaqueness of such systems.[76] However, we have identified that the work of activists and journalists has been able to, with limited exposure, raise a critical public discussion on these issues.[77] Some of these journalistic investigations have, for example, led to questions being asked to the Danish Ministry of Justice by the Parliament.[78]

---

74. Winston, Ali. 'Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology.' *The Verge*, 27 February 2018. https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd; 'NoTechFor: Forced Assimilation.' *No Tech For Tyrants*, 13 July 2020. https://notechfortyrants.org/2020/07/13/notechfor-forced-assimilation/.

75. Ibid. footnote 70

76. Jesper Lund (IT-Pol Denmark) in personal communication with the authors, May 2022.

77. Kulager, Frederik. 'For fire år siden fik politiet et "supervåben". Her er, hvordan det har transformeret ordensmagten'. *Zetland*, 4 May 2021. https://www.zetland.dk/historie/sO9kBG7W-aOZ-j67pz-04ca0; Hoff-Lund, Ole. 'Forskere sætter kritisk fokus på politi-teknologier'. *PROSA*, 3 February 2021. https://www.prosa.dk/artikel/forskere-saetter-kritisk-fokus-paa-politi-teknologier/; 'Forskere sætter kritisk fokus på politiets datadrevne værktøjer.' *Dansk Politi*, 5 February 2021. https://dansk-politi.dk/nyheder/forskere-saetter-kritisk-fokus-paa-politiets-datadrevne-vaerktoejer.

78. For example, see this question submitted by the Danish Parliament to the Justice Minister in May 2021, asking about the use of Palantir after reporting from *The Guardian*: https://www.ft.dk/samling/20201/almdel/reu/spm/908/svar/1777594/2385685/index.htm

5 Analysis

The seven case studies of police abuse of power enable us to reflect on a few key dynamics.

MYTH OF PROTECTION THROUGH EFFICIENT SURVEILLANCE TECH

Across the cases it becomes visible how surveillance technologies are presented as ways for police to address existing issues in society, increasing the security and protection of citizens. This is an extension of the underlying myth that resourcing more policing will make society safer and solve social problems. Often, this involves justifying the deployment of technology in terms of efficiency and cost-effectiveness. In the case of Denmark and Palantir, marketing promises were made in the purchase of the system, though in fact the promises made are actually not possible. In the Brazil case, the heavy investment in surveillance technology is justified as an intervention in the name of security, deployed at scale to the detriment of already marginalised and over-policed communities.

Across cases, the "threats" that policing, and by extension surveillance technology, supposedly keep us safe from, differ. However, in many cases, the myth of policing as protection is deployed to protect against marginalised communities: in the Denmark case, racialised "terrorists"; in Brazil, racialised and criminalised favela communities; in India, members of scheduled castes and scheduled tribes.

FOR PROFIT NOT PEOPLE

An immediate counterpoint to the myth of protection described above is that there is a clear incentive to profit. Despite the myth of protection outlined above, a consistent theme across multiple cases is how a profit-driven surveillance industry distorts the incentives of policing. Perhaps the most blatant example of this was the Thames Valley Police partnership with the reality TV show Road Wars, in which the police were paid for footage collected by (among other devices) car dash cams. The

need to create interesting or entertaining content could certainly unduly influence policing methods.

Alternatively, in many of these cases, a powerful private company (such as Palantir or the NSO group) is marketing their systems directly to the police to buy their systems. This draws on the myth of protection, which companies can use to sell more technology. Collaborations with the private sector which introduce a profit motive to ever expanding technology-driven data collection benefit the surveillance industry and not the public. Such partnerships can lock public administration into contracts which limit democratic bodies' ability to turn off surveillance devices or delete their data, as in the case of the San Diego streetlights.

FUNCTION CREEP

'Function creep' occurs when technologies developed for one specified purpose (perhaps in the public interest) are co-opted for surveillance or profit. Perhaps the most visible case of function creep is the San Diego case, as the original goal of the "smart" streetlights (smart city energy saving) was completely different from the goal it ended up being used to (collecting video footage for the Police). This shows a dynamic through which the police progressively broadens its surveillance reach. For example, first the video footage is only used for "serious crime,", then to other forms of criminal activity as well.

A slightly different form of function creep is the case of the UK police officers' use of databases for personal stalking. There, function creep exists, as officers access data that was intended for a different purpose, but it is an illegal activity. The case further reinforces the idea that once surveillance structures are deployed, they carry with them the potential for future abuse, often in forms that could not have been predicted initially. Another example of this is the Thames Valley Police use of dashcam footage. A technology which was initially intended for police accountability becomes fodder for reality TV. Technologists should proactively account for function creep in their designs, and limit unnecessary data collection: for example, in the San Diego case, they could advocate for the use of other sensing tech instead of cameras which would be harder to abuse, questioning why smart streetlights even need cameras in the first place.

INCENTIVISING DATA COLLECTION

Another aspect of function creep is the way the implementation of surveillance technology incentivizes further data collection. An example of this is the case of Palantir in Denmark. Once the system is set up to connect previously-siloed databases, further integrating and collecting more data can become a goal of policing institutions. Although the police might not know what to do with such data, there is an imperative for generating and collecting more data, often without a clear end goal. An element of this may be that the police need to justify the purchase of such surveillance technology. There is an incentive to just try and apply the technology at any cost in order to justify the budget for it and future ones too.

A consequence of this, as seen in the case of Pegasus in Mexico, is that once the state has the technological power to surveil people, they increase their scale of surveillance and data collection. Once the software was developed and put into operation, though illegally, it generates the conditions for further breaking the law and collecting more information.

EMBEDDING POWER AND MARGINALISATION

In each case we examined, surveillance technology targets and disproportionately harms already marginalised populations, furthering social inequality and reinforcing power imbalances between police and people. Local contexts and local histories of policing matter to understand the dynamics these technologies reinforce once they're implemented.

In Brasil, video surveillance technologies are deployed without oversight or regulation in a region (the Jacarezinho *favela*) where a historically marginalised community resides. In the UK, police databases are used by police perpetrators of domestic abuse to further control their intimate partners in a process that continues a history of institutional sexism and gender-based violence. In Denmark, the myth of predictive policing focuses police surveillance on neighborhoods which are also being targetted by a "ghetto package" targetted at "non-Western Danes" in an openly racialised and Islamophobic policy agenda. In each of these cases, marginalised communities also develop methods of resistance to avoid and challenge surveillance.

SECRECY AND OBFUSCATION

Surveillance technologies are often introduced in secret, and their use is often obfuscated. In the case of San Diego, surveillance cameras were built into streetlights without the knowledge of either council members or residents. Police began accessing footage from these cameras long before civil society groups and city council leaders were even aware these cameras existed. In Mexico, the purchase and use of Pegasus was initially secret before it was exposed by leaks and journalistic investigations. As the different cases show, various concerns may be used as a pretext to keep these technologies secret, such as national security, cybersecurity, as well as the trade secrets of involved companies. Such secrecy is inherently abusive, but it also enables further abuses, as civil society and lawmakers cannot challenge the use of technology they do not know about.[79] Even when laws exist to prevent such uses, keeping them out of the public focus ensures they remain in place.

---

79. Slupska, Julia, Jeanette Lowrie, Lilly Irani, and Deian Stefan. 'How Secrecy Leads to Bad Public Technology'. *UC San Diego*, 28 June 2021. https://escholarship.org/uc/item/89d7826n;

LACK OF ACCOUNTABILITY

Cases of police abuse using surveillance technology are consistently difficult to bring to justice. In Mexico, there have been no sackings over the Pegasus revelations, despite forensic evidence showing the software had been widely used to target government critics, over USD 160 million spent on the technology. In cases like Denmark, Mexico, or India, where the law permits these uses of surveillance technology, there are no clear routes for seeking accountability. Even in cases like UK police domestic violence, where the abuse is made public and obviously illegal, insufficient accountability mechanisms prevent survivors from seeking justice. Police officers' ability to access their own criminal files points to failures of accountability that are deeply embedded within the system.

Furthermore, surveillance technology itself can be used to dodge attempts at accountability. In the case of Brazil, this is quite clear in how the police decide to increase surveillance instead of dealing with the underlying issues of police abuse. These systems are implemented without oversight and, though clearly problematic, there is very limited reaction from institutions. Similarly in Thames Valley, technology implemented using the pretext of police accountability (i.e. police dashcams) is repurposed as a source of content for entertainment, profit and propaganda.

LAWS ARE NOT ENOUGH

This report shows the failure of laws and legal institutions to curtain police abuse of surveillance technology. Indeed, in some cases, laws have enabled unaccountable police actions, and enabled and legitimized the abuses of power highlighted in this report. These cases show that reference to the legal legitimacy of police action does not always vindicate its political or ethical legitimacy.

Even in situations where there is manifest illegality and failure to comply with legal standards (for example, for police procedure, privacy law, administrative law, or data protection law), there is a failure of institutional accountability in taking cognizance of these matters, and a failure of legal and political institutions (for example, courts or police conduct tribunals) in responding to possible breaches of the law. In many cases, legal and institutional mechanisms for accountability and redress of police abuse are simply too costly, too time consuming, or too difficult for aggrieved persons to resort to without adequate support. This indicates broader structural failures in how legal institutions are set up to respond to police abuse, so that even where there are potential violations of the law by the police, there are few avenues to hold them accountable or provide redress.

Laws and legal institutions do not adequately protect against police abuse of power through surveillance technologies—not just because the right laws haven't been passed, but also because in many cases, existing laws and legal institutions protect police and are at a structural level shaped by the same social systems of domination (e.g. white supremacy) reproduced in police abuse of power. Although calls for legal reform or institutional oversight can be useful strategies depending

on local context, ultimately legal justifications for police power must be more carefully interrogated and constantly challenged with a lens towards abolitionist practice and "non-reformist reforms" for curtailing police abuse.

RESISTANCE AND ABOLITION

Across all the cases it was possible to identify people and institutions resisting police abuse of power. Many different modes of resistance can be highlighted, including raising awareness (through journalism/research), monitoring police activity, calling for oversight mechanisms, launching complaints, solidarity groups, direct action, and protests. This very report was only made possible thanks to the effort made by many civil society groups globally that publicly documented these cases—several of which we connected within our workshop.

The work of civil society actors to monitor and act against police abuse of power and technology assumes many uncertainties, risks, and coordination between separate entities. In the case of illegal abuse of power, for example, these groups are required to actively monitor police activities, interact, and learn from the people that were on the receiving end of these activities and potentially investigate cases in order to uncover abuse. An example of this is the case of Pegasus in Mexico, which required years of investigative efforts from tens of people and institutions. In contrast, legal abuse of power may be more visible and identifiable, but also particularly difficult to act against, as they require starting a conversation on the legality of such practices and challenging established norms. Moreover, once populations consent to surveillance technologies being used in their communities, it may be hard to resist their further use.

On a whole, however, our suggestion from looking at these cases from an abolitionist viewpoint is that it is not just about fixing surveillance tech systems so they're "fair," to collect "better" data, or create "better" technology design. A key goal should be avoiding the expansion of police surveillance as a whole, thus severely controlling their use or abolishing them altogether. In sum, it is about the goal of defunding and abolishing both police and the surveillance industry which thrives from it. We hope that the global perspective taken by this report can support and enable local action in this regard.

6 Conclusion

Our analysis of seven case studies across six national contexts articulates an underlying logic by which surveillance technology enhances police abuse of power. Purchases of surveillance technology are justified using a *myth of protection*: i.e. that technology will ensure the police can protect the public against crime more efficiently and fairly (expanding another myth that more police powers equals more protection). However, these purchases are motivated by and accountable to profit-seeking markets rather than democratic accountability, which benefits the surveillance industry and not the public.

Once purchased, these technologies incentivise ever expanding data-collection, resulting in "function creep" towards ever more pervasive surveillance. Across various contexts, this surveillance disproportionately targets those who are already marginalised on the basis of race, class, gender, and/or caste. Resistance is challenging because the technologies are often purchased and deployed in secret, and even when they are exposed through leaks or investigations, police often act with impunity in a landscape of limited regulatory oversight. However, in each case we examined resistance is taking place in various forms: through documentation, legal actions, and challenging the underlying structures of police powers and the surveillance industry.

We call others to action to prevent public private partnerships from perpetuating structural violence.

In highlighting these efforts, we wish to support them and call others to action to prevent public private partnerships from perpetuating structural violence. By challenging police use of surveillance technology, we can reduce sweeping police powers and by extension the types of harms and abuse we identify in this report. Thus, we call on fellow researchers, civil society, and technologists to divest from surveillance technology and policing, for example:

RESEARCHERS: Stop recommending intrusive surveillance and repressive policing as solutions to social problems. Aim instead for research towards a generative, abolitionist project for a world where surveillance technology isn't necessary.

TECHNOLOGISTS: Avoid developing technology which expands police powers. Refuse the development of surveillance technology, embedding an abolitionist approach in your practice. Whenever possible, consider function creep and other long-term impacts of technologies whenever they are developed.

CIVIL SOCIETY: Campaign for greater democratic oversight and community accountability measures on police purchase and use of surveillance technology, in line with the aim of reducing police power.

We thank the following individuals and organisations for their feedback and input on the report:

Alex Argüelles, Member of Comun.al

Anushka Jain (she/her), Associate Policy Counsel (Surveillance & Transparency), Internet Freedom Foundation

Seeta Peña Gangadharan, Associate Professor, London School of Economics and Political Science

Pablo Nunes, PhD in Political Science and Coordinator at the Center of Security and Citizenship Studies (CESeC)

Criminal Justice and Police Accountability Project (CPA Project)

Homo Digitalis

Jesper Lund, IT-Pol Denmark

NO TECH FOR TYRANTS

7 November 2022

About No Tech For Tyrants

No Tech For Tyrants (NT4T) is a collective of organisers, students and researchers working to disrupt actors and processes that house and enable violent tech. Primarily based in the United Kingdom, we coordinate research; host teach-ins, talks and workshops; and conduct public campaigns in order to dismantle the violence infrastructure at the intersection of technology, migration governance, and surveillance.

Contact Us

Website: www.notechfortyrants.org
Twitter: @NoTech4Tyrants

Design Flávia Castanheira
Illustrations Jônatas Moreira