Merykokeb Belay

Mary Kryslette Bunyi

Maryam Khalid Shah

**Case Analysis:**

**Using Facial Recognition Technology (FRT) for Law Enforcement**

The South Wales case sheds light not only on the future direction of the use of AFR technologies in the United Kingdom, but also on the dynamics of policing efforts in the region. On one hand, various citizens and civil society groups have raised concerns not only about the current use of AFR, but of its sinister potential if allowed to further develop in the policing space. There are growing fears of the potential for governments to use AFR to target opponents, quell dissent, or make unlawful arrests[[1]](#footnote-1). There also are fears of ‘mission creep’, where AFR might open pathways for authorities to gradually adapt the tools to further impinge on privacy rights[[2]](#footnote-2). On the other hand, AFR Locate was an illustration of the disconnect between the authorities’ judgment of priorities and worthy trade-offs vis-à-vis broader community implications. The conception and implementation did not consider community cohesion. While the motivation in the technology’s acquisition was to safeguard the general public’s security more effectively, the community’s lack of voice in the process may have led to low public trust and a heightened feeling of insecurity.

**Policy Context**

The case illustrates the contrast between the police and the policed. Value-setting was performed mainly by public officials who framed the issue as one of inflicting private harm for the greater public good. The Court of Appeal was satisfied that AFR Locate constituted “proportionate interference”, finding that the initiative’s flaws mainly revolved around its governance[[3]](#footnote-3). The SWP viewed AFR Locate as a tool to improve organizational performance, whereas NEC, being a private contractor, was motivated by profit maximization. These contexts led the SWP to narrowly focus on the technology’s potential for police efficiency without investigating the workings of the algorithm or considering community-wide implications, while NEC focused on delivering the product in a black-boxed manner to retain proprietary control over it and was not concerned with a proper hand-off process.

The consequences of the policy actors’ siloed values and narrow goals were manifested in the resulting hit to community cohesion and lack of operator engagement. First, the public had no choice but to give up their privacy when they attend events where the AFR Locate is deployed, without any mechanisms for consultation or feedback. Increased public insecurity from privacy and bias issues went against the intention of SWP to use AFR Locate to ensure public security. Second, the operators were noted to be lacking in training and engagement due to the sheer number of false positive matches in the program’s initial deployment[[4]](#footnote-4). Improvements were largely reactionary and set off after the problems encountered in the Champions’ League deployment and findings released in the court ruling[[5]](#footnote-5). The AFR Locate case showed a lack of consideration for broader contexts, failing to institute measures accounting for user and subject implications.

**Issue Diagnosis**

The issues presented in this case can be diagnosed as lacking public participation and accountability. The public, in this context, refers to citizens that were subjected to the technology (attendees of the Champions League, for example) and operators that shouldered the responsibility of validating AFR Locate. With regards to adopting AFR Locate in policing, SWP’s decision making process was siloed and hierarchical in nature; it excluded operators, stakeholders, and community members. By limiting decision making processes to senior officers, SWP took away the public’s agency to question/criticize the need for AFR and, thus, hold SWP responsible for the implications of this decision. This makes it difficult to ascertain where ownership ends once the technical specifications of the end product are met. And, perhaps more importantly, where responsibility is placed when the software results in false positives. As Ed Bridges notes, the lack of public accountability made it so that there was no way for concerned citizens to challenge the use of the technology except through courts. In adopting a reactionary stance towards public concerns and criticisms, SWP ensured that the outcomes of this project would not be equitable. As Katel et al. note, equitable processes are what determine equitable outcomes—SWP’s approach was far from equitable as it lacked the basic tenets of participatory design[[6]](#footnote-6). They failed to create an inclusive and collaborative environment where the public could contribute to decisions; voice concerns; and provide actionable insights that may not have been obvious to the police force.

**Ethical Questions**

In moments of decision-making presented by the case, various questions around algorithmic accountability and equity need to be considered. We want to understand who defined the problem that AFR Locate was acquired to address. Did the criteria such as cost effectiveness and quality that was used to determine NEC as the contract winner reflect issues about who was involved? Related to this, we also want to examine whether algorithmic bias was a concern of SWP while acquiring AFR Locate, and how effectively and transparently law enforcement agencies can use black-box technologies. Moreover, who is held responsible if an AFR Locate operator does not alert intervention teams of a positive match? For instance, if an operator has to quickly go through hundreds of matches (as they did at the Champions League Final), and fails to accurately verify a person that goes on to commit a crime, who is responsible? Would SWP be to blame, or would there be a “moral crumple zone” where the integrity of AFR Locate would be protected at the expense of the operator[[7]](#footnote-7).

One of the main questions that arises about working with data in this particular case is of data collection, specifically with regards to the dataset used to train algorithms e.g. M20 in AFR Locate. With training datasets that do not adequately represent everyone e.g. lesser representation of darker skinned individuals in AFR Locate, can positive efforts such as reducing crime lead to essentially discriminatory behavior e.g. SWP checking IDs of more darker skinned people? It also leads to the question of whether an auditing for bias by the developer of an algorithm is enough or is an independent evaluation required, as well as whether acquirers of AFR technology should be allowed to adopt the technology without conducting their own rigorous testing and statistical validation studies[[8]](#footnote-8)? Moreover, SWP’s poor quality watchlist images that resulted in some people becoming frequent ‘hitters’ highlights the importance of data collection and prompts us to examine the balance between, and effects of, using poor quality data entries versus eliminating them. We also need to think about the tradeoff between accuracy and interpretability/transparency of machine learning algorithms, especially in a social context involving law enforcement agencies.

**Our Reflections**

In analyzing this case, we were made acutely aware of how decision-making processes determine outcomes. As data scientists, we are constantly having to make decisions on how we collect; analyze; and interpret data. In addition to technical considerations, our preconceived assumptions and lived experiences play a key part in what we decide to flag as an issue and what we overlook. Often, these pivotal considerations are made in isolation or amongst a team of like-minded practitioners. This case has highlighted how such siloed and isolated processes allow biases and assumptions to go unchecked by excluding stakeholders specializing in non-data science fields. Additionally, using the concept of ‘the moral crumple zone’[[9]](#footnote-9), we reflected on where blame should/would be placed—are the SWP operators the main party to blame for the failings of AFR Locate? Could they also be considered victims of ‘the moral crumple zone’, given that they are implementing higher authorities’ visions and being on the receiving end of NEC technologies that they do not necessarily understand? Lastly, our analysis was a product of continued deliberation on each group members’ preconceived ideas about safety/security and public agency. Although we unanimously agreed that decisions such as the one SWP made require wider public transparency and accountability, we initially struggled to determine to what degree communities should have a say in how they are monitored.

Is there ever a security threat/situation that would justify the implementation of AFR-type technologies without incorporating participatory design frameworks?

**Proposed Course of Action**

The case highlights the importance of stakeholder engagement and inclusion in the policy development processes. This is encapsulated in Ed Bridges’ statement that bringing the case to the court was the only way they could challenge the use of the technology. The police’s approach to AFR Locate was centered on legal compliance and public acquiescence. However, the case highlights the importance of stakeholder trust as well as community empowerment in surveillance policymaking. The public should not be treated as a bystander without any agency. The public is entitled to more than information that they will be subject to facial biometric scanning by an AFR Locate van. In the spirit of participatory design, the application and evaluation of the technology must first and foremost be situated in the context of the affected communities[[10]](#footnote-10).

We believe the most promising, necessary, and plausible option is to invest existing resources towards ensuring sustained and meaningful engagement with low-ranking officers/AFR operators in the police force and local community members. As mentioned earlier, this case is plagued with hierarchical decision making, which is the root cause of its issues. By purchasing AFR Locate, SWP had misguidedly anticipated seeing improvements to community cohesion by way of increased public safety. However, experts in community activism and community policing have found that pouring investments into technologies like AFR rarely improves social capital and does little to build community cohesion[[11]](#footnote-11). Rather, we believe that ensuring public safety requires a bottom-up approach, much like the process used by Katel et al. in developing the Algorithmic Equity Toolkit[[12]](#footnote-12). Adopting a community-centered approach that facilitates input from all concerned citizens will have a more impactful effect on community cohesion and public safety.

Our articulation of the issue shows that other actors and stakeholders in the policy environment need to be collaborated with in order to achieve the best outcome. This could mean utilizing the technical skills and expertise of other policy actors, or creating a space where an exchange of ideas, feedback, and criticism can take place. Without the involvement of other stakeholders, one would have only a myopic view, resulting in only a partial understanding of the issue.

**Role as Data Experts**

With regards to our positionality as data experts, we should work towards making the process of working with data more accessible to non-experts. By explaining technical aspects of a system in layman terms, we can ensure wider public understanding and more effective participation in the decision-making process. Moreover, we should welcome feedback and criticism from non-experts in order to build a collaborative relationship and foster trust. As data experts, it is also our responsibility to be transparent about the data we are working with as well as our processes of collecting and working with it, which includes being more forthcoming about all of the small choices that shape our decisions and systems[[13]](#footnote-13). Drawing from the recent case of Dr. Timnit Gebru, this includes prioritizing honesty and transparency about biases in technologies as well as about possible harms that a technology could have.

**Our Backgrounds**

Despite different backgrounds and forms of expertise, we could identify commonalities in terms of everyone realizing the need for data experts to be more forthcoming with their decisions, and the importance of stakeholder engagement. One team member’s experience of working with different stakeholders in a low-income community helped us to understand the power of shared goals and collaboration. Another drew on her experience of using data as a motivation tool while working as a public school teacher while thinking about the importance of interpretability in machine learning algorithms. Another team member with law enforcement background rounded the group’s approach to consider the governmental perspective.

**Resources and Constraints**

As with most public policy proposals, the openness of decision-making authorities to implement the proposed initiatives would be a key factor to success. In this case, the British philosophy of ‘policing by consent’ may favor the suggested collaborative interventions, as this will be an avenue for the public to concretely set the boundaries of such consent[[14]](#footnote-14). However, a lack of technical expertise may limit communication and public understanding of the technology’s algorithmic equity and implications.

Participatory design methods are only as good as the willingness of its community members to engage. While active members of the community can provide the impetus needed for the public to decisively exercise its voice, collective action is necessary for systemic change to happen[[15]](#footnote-15). Participatory methods may likewise require the patience of the government and community in terms of expending more time and financial resources compared to traditional processes. In the words of anti-carceral organizer Sarah Hamid, “We need to make sure that the tools we are using are safe for our communities. So we can’t move too fast. We have to be slow, and difficult, and deliberately endure the drag”.[[16]](#footnote-16)

**Importance of Public Participation**

In sum, the South Wales case illustrates not only the debate surrounding AFR technologies and privacy rights in the United Kingdom, but more importantly, the power dynamics between the policed and the police. The case highlights the importance of public empowerment in the policy development process. Especially when essentially contested concepts such as privacy are involved, mechanisms ensuring public accountability and public trust are paramount so that technologies are used for the right purpose and in the right manner[[17]](#footnote-17).

**Bibliography**

Bethan, Martin, and Andrew Dawson. *An Evaluation Of South Wales Police’s Use Of Automated Facial Recognition*. Cardiff University, 2018.<https://crimeandsecurity.org/s/AFR-Report-Digital.pdf>.

D. K. Mulligan, C. Koopman, & N. Doty. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160118.

Huang, Karen, “Privacy and Surveillance”. Lecture for PPOL568 (Data Ethics), Georgetown University, Washington, D.C., February 10, 2021.

Huang, Karen, “Data Ethics in Practice”. Lecture for PPOL568 (Data Ethics), Georgetown University, Washington, D.C., March 10, 2021.

J. Angwin, J. Larson, S. Mattu, and L. Kirchner. “Machine Bias: There’s software used across the country to predict future criminals. And it’s biased against blacks”. *ProPublica*, May 23, 2016. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

Kaltheuner, Frederike. “Facial recognition cameras will put us all in an identity parade”. *The Guardian*, January 27, 2020. <https://www.theguardian.com/commentisfree/2020/jan/27/facial-recognition-cameras-technology-police>

Logic Magazine. “Community Defense: Sarah T. Hamid on Abolishing Carceral Technologies”. Issue 11 Care, 2020.

Lomas, Natasha. “Court finds some fault with UK police force’s use of facial recognition tech”. *TechCrunch*, August 2020. <https://techcrunch.com/2020/08/11/court-finds-some-fault-with-uk-police-forces-use-of-facial-recognition-tech/>.

M. C. Elish, “Moral Crumple Zones: Cautionary Tales in Human-Robot Interactions”. *SSRN*, April 3, 2016. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757236>.

M. Katell et al. (2020). “Toward Situated Interventions for Algorithmic Equity: Lessons from the Field.” *ACM Conference on Fairness, Accountability, and Transparency (ACM FAccT\*)*.

R (on the application of Edward Bridges) v. The Chief Constable of South Wales POLICE, C1/2019/2670 (EWCA Civ 1058, August 11, 2020).

Roussi, Antoaneta. “Resisting the rise of facial recognition”. *Nature*, November 18, 2020. <https://www.theguardian.com/technology/2020/aug/11/south-wales-police-lose-landmark-facial-recognition-case>.

S. Barocas and D. Boyd. “Computing Ethics: Engaging the Ethics of Data Science in Practice”. Communications of the ACM, Vol. 60 No. 11, Pages 23-25. <https://dl.acm.org/doi/fullHtml/10.1145/3144172>.

Shead, Sam. "UK Court Finds Facial Recognition Technology Used by Police Was Unlawful." *CNBC*, August 20, 2020.<https://www.cnbc.com/2020/08/11/swp-facial-recognition-unlawful.html>.

UK Government. "Definition of Policing by Consent." December 10, 2012. <https://www.gov.uk/government/publications/policing-by-consent/definition-of-policing-by-consent>.

1. Roussi, Antoaneta. “Resisting the rise of facial recognition”. *Nature*, November 18, 2020. [↑](#footnote-ref-1)
2. Kaltheuner, Frederike. “Facial recognition cameras will put us all in an identity parade”. *The Guardian*, January 27, 2020.

   Huang, Karen, “Privacy and Surveillance”. Lecture for PPOL568 (Data Ethics), Georgetown University, Washington, D.C., February 10, 2021. [↑](#footnote-ref-2)
3. R (on the application of Edward Bridges) v. The Chief Constable of South Wales POLICE, C1/2019/2670 (EWCA Civ 1058, August 11, 2020). [↑](#footnote-ref-3)
4. Bethan, Martin, and Andrew Dawson. *An Evaluation Of South Wales Police’s Use Of Automated Facial Recognition*. Cardiff University, 2018. [↑](#footnote-ref-4)
5. Bethan, Martin, and Andrew Dawson. *An Evaluation Of South Wales Police’s Use Of Automated Facial Recognition*. Cardiff University, 2018. [↑](#footnote-ref-5)
6. M. Katell et al. (2020). “Toward Situated Interventions for Algorithmic Equity: Lessons from the Field.” *ACM Conference on Fairness, Accountability, and Transparency (ACM FAccT\*)*. [↑](#footnote-ref-6)
7. M. C. Elish, “Moral Crumple Zones: Cautionary Tales in Human-Robot Interactions”. *SSRN*, April 3, 2016. [↑](#footnote-ref-7)
8. J. Angwin, J. Larson, S. Mattu, and L. Kirchner. “Machine Bias: There’s software used across the country to predict future criminals. And it’s biased against blacks”. *ProPublica*, May 23, 2016. [↑](#footnote-ref-8)
9. M. C. Elish, “Moral Crumple Zones: Cautionary Tales in Human-Robot Interactions”. *SSRN*, April 3, 2016. [↑](#footnote-ref-9)
10. M. Katell et al. (2020). “Toward Situated Interventions for Algorithmic Equity: Lessons from the Field.” *ACM Conference on Fairness, Accountability, and Transparency (ACM FAccT\*)*. [↑](#footnote-ref-10)
11. Logic Magazine. “Community Defense: Sarah T. Hamid on Abolishing Carceral Technologies”. Issue 11 Care, 2020. [↑](#footnote-ref-11)
12. M. Katell et al. (2020). “Toward Situated Interventions for Algorithmic Equity: Lessons from the Field.” *ACM Conference on Fairness, Accountability, and Transparency (ACM FAccT\*)*. [↑](#footnote-ref-12)
13. S. Barocas and D. Boyd. “Computing Ethics: Engaging the Ethics of Data Science in Practice”. Communications of the ACM, Vol. 60 No. 11, Pages 23-25. [↑](#footnote-ref-13)
14. UK Government. "Definition of Policing by Consent." December 10, 2012. [↑](#footnote-ref-14)
15. Huang, Karen, “Data Ethics in Practice”. Lecture for PPOL568 (Data Ethics), Georgetown University, Washington, D.C., March 10, 2021. [↑](#footnote-ref-15)
16. Logic Magazine. “Community Defense: Sarah T. Hamid on Abolishing Carceral Technologies”. Issue 11 Care, 2020. [↑](#footnote-ref-16)
17. D. K. Mulligan, C. Koopman, & N. Doty. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160118. [↑](#footnote-ref-17)