medConfidential — Written evidence (NTL0050)

1. There are precedents in the use of (even basic) technologies by organisations that are seen to be so institutionally untrustworthy by a meaningful segment of the population that they are not allowed *by law* to use computers to make records searchable, cf. the National Trace Centre,[1] for gun sales in the United States.

2. We hope the degradation in trust in policing and technology in the UK does not go that far. That will, however, require actions from the police – and more importantly, policy from the Home Office – that we have seen no sign either are willing to consider. medConfidential therefore warmly welcomes the creation of this committee, and this inquiry.

Examples from health innovations and technologies

3. It is a Whitehall truism that 'the NHS is bad with new technology', but – as with many Whitehall truisms – it is not actually true. The reason why it is not provides an illuminating example for law enforcement uses of technologies.

4. Every doctor uses technology that helps their patients, once it is shown to work, and once they believe it works,[2] and as long as it works in line with their Hippocratic Oath.[3] Whether higher level institutions (especially in Whitehall) are aware is not relevant to individual doctors – end-to-end encrypted messaging protected your doctor's medical communications before NHS England had any guidance on it.

5. Police officers probably began creating WhatsApp groups around the same time as doctors did. The police don't have a Hippocratic Oath, but they are incentivised to minimise crime – whether by solving it or not recording it – and the technologies they find useful will similarly be used.

6. In law enforcement, absent a Hippocratic Oath, that technology innovation has included the copying of each rape victim's entire mobile phone contents and social media history.

7. Given the technology was available, it was logical for the police to routinely do so – and equally logical for the system to reject cases where they did not. But in this and in other cases, the logic of law enforcement did not seem to take account of the victims.

8. A health system would rightly see that as abhorrent.
9. In health, the names Harold Shipman,[4] Andrew Wakefield[5] and Simon Bramhall[6] are synonymous with system change, after their actions caused

---

[1] https://www.thetrace.org/2016/08/atf-non-searchable-databases/
[2] These are not exactly the same thing.
[3] In the UK, the modern 'Hippocratic Oath' is the core values and principles set by the General Medical Council, laid out as the ethical duties of a doctor in "Good Medical Practice" (2013).
[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/ 228886/7014.pdf
[5] https://www.bmj.com/press-releases/2011/11/09/mmr-fraud-needs-parliamentary-inquiry-says-

harm. By contrast, the actions of Simon Harwood,[7] Wayne Couzens[8] and Bob Lambert,[9] seem to have resulted in no systematic change; and arguably no change at all.[10]

10. Any choice to give law enforcement access to advanced technologies must recognise and account for the culture and processes within which those technologies will be deployed. What the Independent Inquiry into the death of Daniel Morgan termed "institutional corruption", institutional racism, and the ability to deprive a person of freedoms or money is a toxic combination.

11. The "innovations" of Tuskegee are looked back on with horror in the health world, and in the wider community they contribute to vaccine hesitancy to this day. It is unclear what the policing equivalent of Tuskegee would be – the murder of Ian Tomlinson? – and what regular "bobbies on the beat" would say about the harms and lessons of that event.[11]

12. Policing must, of course, use novel technologies in delivering its mission. ANPR[12] may be a good example of such a utility, but the "Royston Ring of Steel" shows how a "proportionate" technology can be used in a way which has no proportion at all. The police had lost their way.

a. The proposed expansion of the Ultra-Low Emissions Zone around London to the North & South Circular Roads, and the process for determining which locations should have policing purposes added, may make for an interesting evidence session from the Committee.[13]

13. Technology enables law enforcement officers and organisations to impact on more innocent people, faster, but the issues around this are never entirely technological. Racists will be racist with or without technology, but technology can make it easier to abuse more people, faster.

When the Home Office found its passport checking algorithm to be racist

14. It is understandable that the Home Office tries new algorithms and new technologies.

15. It is also entirely reasonable that when the process for a new passport allows photos to be uploaded online, an algorithm was built to check those photos against the rules for passport photographs – so if they might be

---

bmj-new- information-puts-spotli
[6] https://www.independent.co.uk/news/uk/crime/simon-bramhall-liver-surgeon-gmc-b1891568.html
[7] https://www.bbc.co.uk/news/av/uk-19626267
[8] https://www.bbc.co.uk/news/uk-england-london-57774597
[9] https://en.wikipedia.org/wiki/Bob_Lambert_(undercover_police_officer)
[10] We could not find a statement that captures in an easy format document what has changed so that members of the public can see quickly those positive changes.
[11] One argument is that of a "single bad apple"; whether the analogy is that, or a spoonful of sewage in a barrel of wine, is a question for another day.
[12] medConfidential sits on the NPCC ANPR advisory group chaired by the Surveillance Camera Commissioner.
[13] We have nothing informative to say on the topic.

rejected, passport applicants could be told sooner, and upload a valid photograph.

16. When the algorithm was shown very clearly to be racist – i.e. it made different decisions for black faces than it did for white ones – the Home Office was notified, and there was significant press coverage.[14] [15] Whether or not the Home Office should have known *before* this happened is an open question.[16]

17. At the point it was clear that the Home Office *did* know, officials said they would look to improve the algorithm. This is the correct response.

18. However, when the Home Office received its upgraded algorithm, *it did nothing with it* – i.e. the Home Office *actively chose to continue using a racist algorithm,* which its officials knew to be racist, in the face of having an alternative.[17]

19. Given this kind of policy 'leadership' from the Home Office, it is unclear whether the police would make any different choices.

20. It would be unreasonable to expect the Home Office to never make mistakes as it tries new things; even if all reasonable steps in consequence scanning[18] are taken to mitigate harms, there can always be something it didn't predict.

21. But, just as we expect our public institutions to install software patches to avoid problems like "WannaCry",[19] it is reasonable to require the Home Office to fix things when fixes are available.

22. That it explicitly chose not to improve a racist algorithm raises policy questions not only on the guidance on technology the Home Office uses itself, but on what it promotes to others.

Lobbying *for* Technologies

23. In many cases, these novel technologies are provided by companies that seek to make money; the more their technologies are used, the more money they make. In the example of messaging above, and irrespective of what doctors were doing, the owners of WhatsApp[20] dispatched their

---

[14] https://www.newscientist.com/article/2219284-uk-launched-passport-photo-checker-it-knew-would-fail- with-dark-skin/

[15] https://www.bbc.co.uk/news/technology-54349538

[16] We understand that a test run using official photographs of members of Parliament was inconclusive, whereas photographs of members of parliament from other countries suggested a racial bias, even when those photos were independently assessed as entirely compliant with the UK passport photograph rules.

[17] https://www.newscientist.com/article/2271078-uk-still-using-racially-biased-passport-tool-despite-available -update/

[18] https://doteveryone.org.uk/project/consequence-scanning/

[19] https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

[20] Facebook

lobbyists to convince the NHS and DHSC that their app be allowed. The app still doesn't meet the specified criteria,[21] but it is on the allowed list for a variety of reasons.

24. Law enforcement (and the Home Office) will similarly be lobbied in public and in private, to try new technologies that will "cut crime" without any burden of accuracy on such statements. And populist Home Secretaries may care more about the response to a press release than to the substantive effects of any technology.[22]

25. COVID-19 shows this to be an endemic problem.

5 October 2021

[21] https://medconfidential.org/2018/instant-messaging-in-clinical-settings/

[22] A key example here would be the "ISIS propaganda detecting AI" built by Faculty Data Science (as now) for the Home Office which had a single purpose of claiming that it was possible; the amount of fiddling of figures needed to make that claim was irrelevant to the claim itself. This works as much for suppliers of technology to the Home Office as it is for technologies developed on behalf of the Home Office.