Twitter Thread by The Citizens

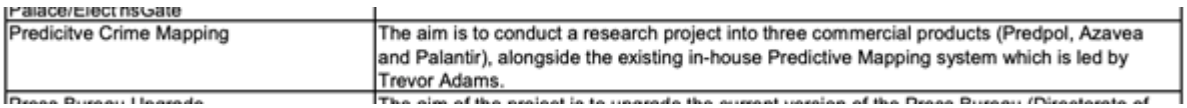
The Citizens
@allthecitizens

Did you catch our thread on the expanding reach of US company Palantir into UK public institutions? £91m+ awarded to the controversial Silicon Valley data-analytics outfit across government. Let's take a look at their work with the British Police…

> Palantir works with the UK police; building highly controversial predictive policing software, gathering intelligence for major sporting events and have also implemented and information sharing initiative across five constabularies, @allthecitizens can reveal. pic.twitter.com/VPZOVuVTpW
>
> — The Citizens (@allthecitizens) January 6, 2021

Between 2014-15 Palantir were 1 of 3 companies trialled by Met police to use an algorithm to consolidate crime data "subject to local interpretation" by police officers, along with PredPol and Azavea.

https://t.co/EfxRHbSQsK



Predicitve Crime Mapping	The aim is to conduct a research project into three commercial products (Predpol, Azavea and Palantir), alongside the existing in-house Predictive Mapping system which is led by Trevor Adams.

This trial was before Data Protection Impact Assessment became a requirement, so it's not known what information was processed, and it took an FOI from @NoTech4Tyrants to even reveal this.

https://t.co/tv1ymD9IMx

In 2019, the BBC reported that at least 14 constabularies in the UK are known to have employed predictive policing software run by companies like IBM, Microsoft, PredPol, and Palantir.

https://t.co/3d3r30jiud

In the US Palantir predictive policing software has been implemented by a number of police departments, notably in New Orleans and by the LAPD, combining datasets in order to map and track criminal activity, surveilling specific people and neighbourhoods.

https://t.co/epzAApvVFC

Predictive policing has raised a number of concerns. Some fear it reinforces police bias and leads to increased police scrutiny in certain areas based on the racial or ethic prejudices of officers:

https://t.co/U1RcGzkWTg

> Yet increasing evidence suggests that human prejudices have been baked into these tools because the machine-learning models are trained on biased police data. Far from avoiding racism, they may simply be better at hiding it. Many critics now view these tools as a form of tech-washing, where a veneer of objectivity covers mechanisms that perpetuate inequities in society.
>
> "It's really just in the past few years that people's views of these tools have shifted from being something that might alleviate bias to something that might entrench it," says Alice Xiang, a lawyer and data scientist who leads research into fairness, transparency and accountability at the Partnership on AI. These biases have been compounded since the first generation of prediction tools appeared 20 or 30 years ago. "We took bad data in the first place, and then we used tools to make it worse," says Katy Weathington, who studies algorithmic bias at the University of Colorado Boulder. "It's just been a self-reinforcing loop over and over again."
>
> Things might be getting worse. In the wake of the protests about police bias after the death of George Floyd at the hands of a police officer in Minneapolis, some police departments are doubling down on their use of predictive tools. A month ago, New York Police Department commissioner Dermot Shea sent a letter to his officers. "In the current climate, we have to fight crime differently," he wrote. "We will do it with less street-stops—perhaps exposing you to less danger and liability—while better utilizing data, intelligence, and all the technology at our disposal ... That means for the NYPD's part, we'll redouble our precision-policing efforts."

LAPD worked with Palantir to create "chronic offender scores" for repeat offenders, leading to individuals being policed based on historic small infractions, such as traffic violations or stop and searches. This led to an increase in targeted individuals being stopped in future.

Of concern too is that, for years, many of these programmes operated in secret, often without even local council members being aware of their existence. It appears the same could now be true in the UK.

https://t.co/py1WWDPYru

@allthecitizens found that the Met trial may not be the only time Palantir has been working with UK police. East Northamptonshire rejected our FOI regarding contracts relating to Palantir under the Section 31 'law enforcement' exemption.

Our response:

I can confirm that East Northamptonshire Council holds the information you have requested, however we are withholding the information as we are consider the information exempt in line with Section 31 (law enforcement) of the Freedom of Information Act 2000.

When considering whether the section 31 Law enforcement can be applied we have to consider the risk of harm as well the public interest in favour of disclosure verses the public interest in favour of non disclosure

Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—

(a) The prevention or detection of crime.

Factors in favour of non disclosure

- Withholding the data enables ENC to better protect .....
- Security of ICT infrastructure, software and systems
- The risk of cyber attacks and incidents, which could have serious consequences for the council and it's residents.
- Commercial interests of any competing companies

Factors in favour of disclosure

- Transparency

This likely refers to a “Transform Police” (T-Police) initiative operated by Northamptonshire, Cheshire, Norfolk, Suffolk Constabularies and the Met, that delivers “intelligence, data integration and situational awareness through Palantir technology”.

https://t.co/0FGZeUbuYt

The initiative seems ostensibly to be a partnership between police forces and tech consultancy Cap Gemini, deploying Palantir technology, “helping intelligence, defence and law enforcement agencies optimize the management and analysis of real data”

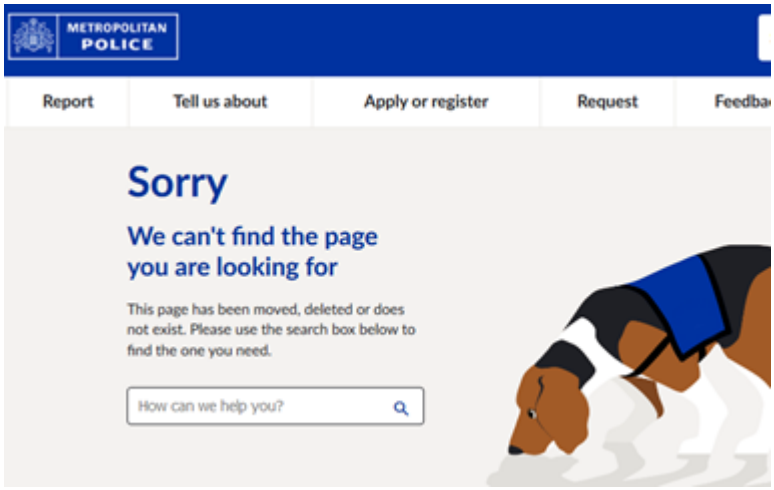
Palantir and Cap Gemini make no secret of working with one another, and have done so since at least 2010. But details of their cross-Police initiative wasn't released under Freedom of Information.

https://t.co/lT6u8VH18Z

It's unclear how many constabularies have bought Palantir's IT help. A promotional video for Cap Gemini/Palantir's T-Police system states "the technology is designed, it's live, we're merely adding more customers to the service that we already provide"

https://t.co/4GsVhmEDYk

Palantir are also "retained on previous plan" under the Digital Policing IT Capital Programme 2016-21, although it's unclear what role they may still have with the Met, and though the archived version of this document is available, it's been removed from the Met Police website.



Palantir were also reportedly involved in a surveillance project with the Police / City of London in 2012, employed to undertake intelligence gathering during that year's Olympic Games.

https://t.co/m8eTn1HtA9

Palantir have maintained engagement with high profile members of the force, meeting with them or hosting events between 2018-2019, including with Cressida Dick and Lancashire Asst. Chief Tim Jacques, and with Mayor's Office for Policing and Crime (MOPAC) going as far back as 2014

3 July	**Hospitality** – London First Dinner/drinks with leading female CEOs Cressida Dick CBE QPM Commissioner Met Police at Palantir, Soho Square, London.	Jasmine Whitbread, Chief Executive London First. Event hosted by London First and Palantir Technologies Inc.	Accepted: key partnership event

What predictive policing work Palantir has undertaken for UK forces remains unclear, but their US and European work could give an indication of the sort of things we might see implemented.

https://t.co/1ePhwbFba1

Palantir UK built sophisticated software for Danish Intelligence Forces (PET) and Police (POL) in the wake of the 2015 Copenhagen terror attacks. The systems could access OS and police databases, social media data, and included hotspot and pattern analysis, and more.

The draft law provides a very general legal basis for combining existing police databases for information analysis in the POL-INTEL system, irrespective of the purpose limitations of these databases, and for collection and processing of information, including personal data, from open sources. The definition of open sources is very broad as it includes any information source which does not require a court order for evidence seizure or interception of electronic communications. The most obvious open data sources are information from the internet and surveillance in public spaces like ANPR, and perhaps facial recognition in the future. However, information that can be purchased from commercial vendors is also specifically mentioned as an open source. This means that the police can buy information on individual citizens from data brokers in Europe, or maybe even the United States, for predictive policing purposes in the POL-INTEL system.

Whatever the true extent of Palantir’s involvement with British law enforcement is - AI, facial recognition, or predictive policing initiatives - the public should know.

If these are systems designed to keep us safe, why the lack of transparency?