

September 2020

All roads lead to Palantir: A review of how the data analytics company has embedded itself throughout the UK

privacyinternational.org

notechfortyrants.org



Authors

This report was compiled by No Tech For Tyrants, a student-led, UK-based organisation working to sever the links between higher education, violent technology, and hostile immigration environments, in collaboration with Privacy International.

Find out more about No Tech For Tyrants: notechfortyrants.org

Researchers:

Mallika Balakrishnan

Niyousha Bastani

Matt Mahmoudi

Quito Tsui

Jacob Zionts

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters: our freedom to be human.

Open access. Some rights reserved.

No Tech for Tryants and Privacy International wants to encourage the circulation of its work as widely as possible while retaining
the copyright. We has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;

We are grateful to Creative Commons for its work and its approach to copyright. For more information please go to www.creativecommons.org.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

No Tech for Tyrants
Notechfortyrants.org/contact

CONTENTS

INTRODUCTION 5

KEY TAKEAWAYS 7

WHO ARE PALANTIR TECHNOLOGIES 8

BACKGROUND 8

PRODUCTS 9

- Gotham 9
- Foundry 10
- Interoperability of products 11

PALANTIR'S RELATIONSHIPS IN THE UK 14

THE NATIONAL HEALTH SERVICE 14

POLICING 20

MINISTRY OF DEFENCE 22

CABINET OFFICE 24

ENTRENCHING INJUSTICE 26

PALANTIR'S GLOBAL RECORD 28

PALANTIR AND THE US 28

- Palantir and the US Department of Health and Human services 29
- Palantir and the US department of Homeland security 30
- Palantir and Project Maven 31

PALANTIR IN EUROPE 32

CONTENTS

PALANTIR AND ISRAEL 33

PALANTIR AND THE WORLD FOOD PROGRAMME 34

PALANTIR'S PRIVACY AND CIVIL LIBERTIES COUNCIL 35

WHERE DO WE GO FROM HERE? 37

HOW DO WE HOLD THE UK GOVERNMENT AND PALANTIR TO ACCOUNT 37

RECOMMENDATIONS FOR THE UK GOVERNMENT 37

ANNEX 1: PALANTIR RESPONSE TO THE REPORT 40

ANNEX 2: PI AND NT4T RESPONSE TO PALANTIR 50

INTRODUCTION

Little known in the UK until the Covid-19 pandemic, Palantir was thrust into the national spotlight in March 2020, when the United Kingdom's National Health Service (NHS) granted Palantir access to unprecedented quantities of health data for processing and analysis in response to Covid-19.

In January of that year, Palantir started working with other governments as well on a series of contracts that would position it as the default platform for expanded health surveillance – justified under the aegis of responding to Covid-19.[1] Palantir claims, in its prospectus[2] to work in over 150 countries in the world. Palantir's contracts with governments around the world have increased in their value to the company markedly over the last two years, up 74% from 31 December 2018 to 30 June 2020 – from $670.6 million to $1.2 billion.[3]

But Palantir's NHS contract is just one of their contracts with the UK government.

Palantir is a name that has become embroiled in controversy. The big-data analytics outfit has morphed into a surveillance behemoth and expanded the capacity of governments to quietly spy on their people.

The company is named after an all-seeing stone in The Lord of the Rings and brands itself as providing similarly ominous powers of surveillance to its clients.[4]

[1] Palantir, Responding to Covid-19, https://www.palantir.com/covid19/.
[2] Palantir, IPO Investment Prospectus, 17 September 2020, https://www.sec.gov/Archives/edgar/data/1321655/000119312520248369/d904406ds1a.htm#rom904406_2.
[3] Palantir IPO Investment Prospectus, 17 September 2020, p 98, https://www.sec.gov/Archives/edgar/data/1321655/000119312520248369/d904406ds1a.htm#rom904406_14.
[4] Canales, K., "Secretive data company Palantir just officially revealed its plans to go public. Here's why it's named after an all-powerful seeing stone in the 'Lord of the Rings'", *Business Insider,* 26 August 2020,

But unlike its fictional namesake, Palantir and its tools may pose a real danger to people in vulnerable positions: the company is known, for instance, for its reported work with US Immigration and Customs Enforcement (ICE), especially under the Trump administration, which is covered later on in this report.[5]

Public private partnerships, like the ones between many branches of the UK government and Palantir, can have a direct and life-altering impact on people's lives. The work that governments do, and the services they deliver, are vital. That's why it is imperative that governments ensure transparency and due process are respected throughout these partnerships.

But, as you will discover throughout this report, transparency is not a frequent feature of these contracts.

This raises questions:

- In what ways will the public's data be used by Palantir?
- What kind of safeguards, if any, were put in place before onboarding Palantir, and subsequently renewing its involvement?
- Who now owns or has access to the public's data, and on what terms?

In creating this report, we set out to explore these questions. We seek greater transparency on how the UK public's sensitive data is being handled and the potential consequences.

https://www.businessinsider.com/what-palantir-name-means-lord-of-the-rings-peter-thiel-2020-7?r=US&IR=T.

[5] Woodman Sp., "Palantir provides the engine for Donald Trump's deportation machine", The Intercept, 2 March 20217, https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/; Mijente, National Immigration Project and Immigrant Defence Project, *Who's Behind ICE? The Tech and Data Companies Fueling Deportations*, 2018, https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf.

KEY TAKEAWAYS

In this report, No Tech For Tyrants and Privacy International (PI) present the findings so far from our collaborative research effort to shed some light on the UK government's extensive and potentially inappropriate links with this tech company.

Palantir, by virtue of being a largely invisible "black box" technology provider, has operated under the radar in the UK until recently.

What we have found:

- **The NHS is not the only UK authority working with Palantir** – the Cabinet Office, the police, and the Ministry of Defence also have had, or currently have, ties with the company. On 22 June 2020, the Home Office told No Tech for Tyrants that they didn't have any contracts with Palantir.[6]
- **The lack of transparency in all of these contracts is a consistent concern.** Both with companies like Palantir, and with any other company the Government is partnering with – particularly this extensively – there should be robust safeguards to ensure transparency and accountability (see Recommendations for the steps we think should be taken).
- In the course of this ongoing research, No Tech for Tyrants and PI have sent 11 Freedom of Information Requests, but received answers to only 4 so far. This is extremely concerning – and points to a broader failure of government to abide by existing regulation and to protect the public's interest.

[6] 'Data processing by Palantir for Home Office' FOI request: https://www.whatdotheyknow.com/request/data_processing_by_palantir_for

WHO ARE PALANTIR TECHNOLOGIES?

BACKGROUND

Founded in 2003 by Peter Thiel (among other co-founders: Stephen Cohen, Gary Tan, Nathan Gettings, Joe Lonsdale (notable for co-founding and currently working as chairman of OpenGov, which deals in cloud-based software for governments), and Alex Karp), Palantir sells data integration and analytics platforms.[7] Its two primary products are Gotham and Foundry (explained further below). One early investor in the company was In-Q-Tel, the CIA's seed funding program – foreshadowing that Palantir's products are often used by national security, defence, and law enforcement agencies.[8]

The potentially deadly consequences of the company's work have been acknowledged – Palantir CEO Alex Karp has, as recently as 2020, made it clear that the company he runs develops tools that are used "to kill people."[9]

The company has gained a reputation for secrecy, and it is often difficult to pin down which governments and companies it works with. This is the case with the UK government as this report demonstrates. While that's not uncommon in

[7] No Tech For Tyrants, "Who's Behind Palantir UK feat. What are They Doing on Your Campus?", 22 October 2020, https://notechfortyrants.org/2020/10/22/whos-behind-palantir-uk-feat-what-are-they-doing-on-your-campus-report-supplement/

[8] Mijente, National Immigration Project and Immigrant Defence Project, *Who's Behind ICE? The Tech and Data Companies Fueling Deportations,* 2018, https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf.

[9] Hamilton, I. A., "Palantir CEO Alex Karp claims the company's tech is used to target and kill terrorists", *Business Insider*, 26 May 2020, https://www.businessinsider.com/palantir-ceo-alex-karp-claims-the-companys-tech-is-used-to-target-and-kill-terrorists-2020-5?op=1&r=US&IR=T.

business, it is and should be uncommon in governments. Yet, governments' dealings with Palantir are often opaque, as this report will seek to make clear.

Palantir has already created a niche for itself in the UK, incorporating several influential figures as stakeholders in the company. These include a peer in the House of Lords[10], a Queen's Counsellor[11] and an, until recently, special consultant to the Home Secretary – who is currently not allowed to lobby the Home Office[12], raising significant concerns about conflicts of interest between Palantir and the public. Read further on "Who's behind Palantir" by No Tech For Tyrants.[13]

PRODUCTS

This section provides a brief review of the primary Palantir products discussed in this report: Gotham and Foundry.

Gotham

Formerly known as Palantir Government, Gotham[14] is designed, in Palantir's words, to "Integrate, manage, secure, and analyse all of your enterprise data."[15] Gotham aggregates the disconnected information storage systems that house an organisation's disparate information sources (e.g. log files, spreadsheets, tables, etc.) into 'a single, coherent data asset."[16] Not only does Gotham

[10] *Register of Interests for Lord Guthrie of Craigiebank—MPs and Lords—UK Parliament*, (n.d.), Retrieved 16 September 2020, from https://members.parliament.uk/member/3608/registeredinterests.
[11] *Sir Daniel Bethlehem KCMG QC*. (n.d.), Twenty Essex, Retrieved 16 September 2020, from https://twentyessex.com/people/daniel-bethlehem/.
[12] *Home Office: business appointment rules advice, October to December 2019* https://www.gov.uk/government/publications/home-office-business-appointment-rules-advice/home-office-business-appointment-rules-advice-october-to-december-2019.
[13] No Tech For Tyrants, Who's Behind Palantir UK feat. What are They Doing on Your Campus?", 22 October 2020, https://notechfortyrants.org/2020/10/22/whos-behind-palantir-uk-feat-what-are-they-doing-on-your-campus-report-supplement/.
[14] Gotham is named after the lawless city in the Batman comics, terrorised by a wide range of villains and criminal interests. A person might wonder if Palantir to what Palantir is comparing itself to.
[15] *Palantir Gotham* (n.d.), Retrieved 16 September 2020 from https://www.palantir.com/palantir-gotham/.
[16] *Ibid*.

make the previously disconnected data more searchable, but it also maps the aggregated data into "…meaningfully defined objects—people, places, things, and events—and the relationships that connect them."[17]

For a breakdown of how ICE uses Gotham, see Mijente and others' "Who's Behind ICE?" report.[18] We also recommend reviewing Motherboard's breakdown of the Gotham user manual obtained via a public record request.[19]

Foundry

Foundry is Palantir's newer, more powerful, and (primarily) corporate-focused version of Gotham. Foundry's primary function is to bring together disparate sources and types of data into a single, accessible platform. According to Palantir's description of how it works,

> "Foundry is a platform that reimagines how people use data by removing the barriers between back-end data management and front-end data analysis. Foundry enables users with varying technical ability and deep subject matter expertise to work meaningfully with data. With Foundry, anyone can source, connect, and transform data into any shape they desire, then use it to take action."[20]

[17] *Ibid*.
[18] Mijente, National Immigration Project and Immigrant Defence Project, *Who's Behind ICE? The Tech and Data Companies Fueling Deportations*, 2018, https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf.
[19] Haskins, C., "Revealed: This Is Palantir's Top-Secret User Manual for Cops", *Vice Motherboard*, 12 July 2019, https://www.vice.com/en_us/article/9kx4z8/revealed-this-is-palantirs-top-secret-user-manual-for-cops.
[20] *Palantir Foundry* (n.d.), Retrieved 16 September 2020 from https://www.palantir.com/palantir-foundry/.

Interoperability of Products

Palantir describes its technology as an "open, interoperable platform designed to maximize the value [one] can derive from [one's] data"[21]. In a Foundry booklet, the company highlights the interoperability of the solution. According to the booklet, "Foundry interoperates with a variety of tools for visualization and analytics, including Palantir platforms" (emphasis added).[22] A Palantir representative explained in an interview that when the company launched Foundry, they "migrated Gotham APIs to modern, interoperable standards [giving] customers the ability to use any tool".[23] Another employee reportedly clarified that "both Gotham and Foundry share the same Palantir DNA: open APIs, fine-grained security and access controls, audit capabilities, interoperability with legacy and 3rd party systems, and cross-organization information sharing to name a few"[24] and that "all data in Gotham can be exported in a variety of open formats, on the front and backends, so that data is never trapped".[25]

Indeed, both products seem to follow the exact same approach regarding data import and export as the relevant product pages found on the UK government Digital Marketplace seem to demonstrate. Below is an example of the data export approach of Foundry. No difference was found between the two products' pages, only the product's name changes:

[21] See 'Palantir: an open technology solution', Palantir website https://www.palantir.com/build/files/An%20Open%20Technology%20Solution.pdf accessed 22 April 2020

[22] See SCRIBD 'Palantir Foundry: Data Management for the Modern Enterprise', page 12 of the 26 of the uploaded document https://www.scribd.com/document/418918675/Palantir-Foundry-Booklet-2, accessed 22 April 2020.

[23] Gourley, B., "An interview with Robert Fink, Architect of Foundry, Palantir's open data platform Part One : Open Data Architectures", *CTOVision.com,* 24 September 2018, https://ctovision.com/an-interview-with-robert-fink-architect-of-foundry-palantirs-open-data-platform-part-one-open-data-architectures.

[24] Gourley, B., "The Titan Release of Palantir Gotham: An Interview with Ryan Beiermeister". *CTOvision.com*, 1 August 2019, https://ctovision.com/the-titan-release-of-palantir-gotham/.

[25] *Ibid.*

> "All data stored in Palantir Foundry [and/or Gotham] is stored in open format, giving an agency complete control over its data and enabling interoperability with other systems. Palantir's open, publicly documented APIs can be configured to import or export to any system that exposes open APIs. There are no limitations on the data that can be exported from Palantir (subject to access controls), and administrators can export data from Palantir in a variety of formats, including but not limited to HTML, Microsoft Office (PPT, DOC, XLS) and ArcGIS (SHP). Data exports can also include the metadata regarding the data's source material references."[26]

In fact, users of both Gotham and Foundry do not even seem to refer to separate tools but rather to a "Palantir platform" that integrates the two solutions.[27] An employee of the Washington DC based Center for Advanced Defense Studies mentioned the existence of a "unified database".[28] In his interview with CTO Vision, Robert Fink, one of the designers of Foundry, confirmed that all the Palantir products share the same database backend called AtlasDB.[29]

Therefore, it appears from the above reports that both tools can process the exact same data in turn. Theoretically the learning

[26] See Gov.uk Digital Marketplace "Palantir Technologies UK, Ltd. - Palantir Gotham", https://www.digitalmarketplace.service.gov.uk/g-cloud/services/660200105725744 ; Gov.uk Digital Marketplace, "Palantir Technologies UK, Ltd. – Palantir Foundry", https://www.digitalmarketplace.service.gov.uk/g-cloud/services/501000199851013.
[27] Bridget Connelly, Environmental Crimes Fusion Cell Analyst, C4ADS: *"The Palantir platform, both through Gotham and Foundry, serves as the foundation to my day-to-day analysis - from ingesting and processing large corporate databases for pattern recognition in Foundry to mapping complex threat networks in Gotham. I can analyze data in Palantir to determine high-level trends in space and time, as well as to identify critical nodes"*, See Palantir Website 'Illicit Networks Uncovered Around the Globe', https://www.palantir.com/philanthropy-engineering/annual-report/2017/c4ads.html.
[28] See *ibid.* Cornelly: *"(…) the unified database allows us to spot points of convergence both within and across projects."*
[29] Gourley, B., "An interview with Robert Fink, Architect of Foundry, Palantir's open data platform Part Three: Open Development Environments", *CTOVision.com,* 1 October 2018, https://ctovision.com/an-interview-with-robert-fink-architect-of-foundry-palantirs-open-data-platform-part-three-open-development-environments/.

system of one could thus be trained with the datasets incorporated in the other, especially when both tools are combined under a single platform.

PALANTIR'S RELATIONSHIPS IN THE UK

In light of the COVID-19 pandemic, Palantir's NHS contracts have received significant coverage in the UK. Our research reveals that Palantir has built relationships with far more entities within the UK Government than just the NHS. In this section, we outline Palantir's connections with the NHS, policing in the UK, the Ministry of Defence, and the Cabinet Office. For Palantir's links to higher education institutions, see No Tech For Tyrants, "Palantir on campus".[30]

THE NATIONAL HEALTH SERVICE

In 2020, Palantir made headlines as one of the companies contracted by the UK government for assistance in its response to fighting the COVID-19 pandemic, specifically for data stores for COVID-19 data (other contracted companies include Faculty, a UK-based artificial intelligence firm that has reportedly previously worked with government officials on Vote Leave[31]).

The NHS reported that they were using Palantir Foundry to manage the front end of their COVID-19 data platform.[32] The first contract in place between Palantir and NHS was valid from 12 March 2020 to 11 June 2020, with a cost to the NHS of £1.[33]

[30] No Tech For Tyrants, "Who's Behind Palantir UK feat. What are They Doing on Your Campus?", 22 October 2020, https://notechfortyrants.org/2020/10/22/whos-behind-palantir-uk-feat-what-are-they-doing-on-your-campus-report-supplement/.
[31] Pegg D., Evans R., Lewis P., "Revealed: Dominic Cummings firm paid Vote Leave's AI firm £260,000", *The Guardian, 12 July 2020* https://www.theguardian.com/politics/2020/jul/12/revealed-dominic-cummings-firm-paid-vote-leaves-ai-firm-260000.
[32] Gould M., Joshi I., & Tang M., "The power of data in a pandemic. Technology in the NHS.", 28 March 2020, https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/.
[33] No Tech For Tyrants, "The Corona Contracts", 7 June 2020, https://notechfortyrants.org/2020/06/07/the-corona-contracts/.

This original contract is in line with the acquisition strategy explained by Palantir in the prospectus they produced proceeding their public listing:

> "In the first phase, we typically acquire new opportunities with minimal risk to our customers through short-term pilot deployments of our software platforms at no or low cost to them. We believe in proving the value of our platforms to our customers. During these short-term pilots, we operate the accounts at a loss. We believe that our investments during this phase will drive future revenue growth."[34]

However, the details of the contracts remain unknown. As of September 2020, No Tech for Tyrants has not received satisfactory responses to its Freedom of Information requests to NHS regarding the scope of data made available to Palantir in this original contract. While Palantir's response to PI and other organisations in May 2020 provided some clarifications, it failed to clarify the extent of the project and what protections exist.[35]

The contract was ultimately extended – from 12 June 2020 to 11 October 2020, and the extension is valued at £1 million.[36]

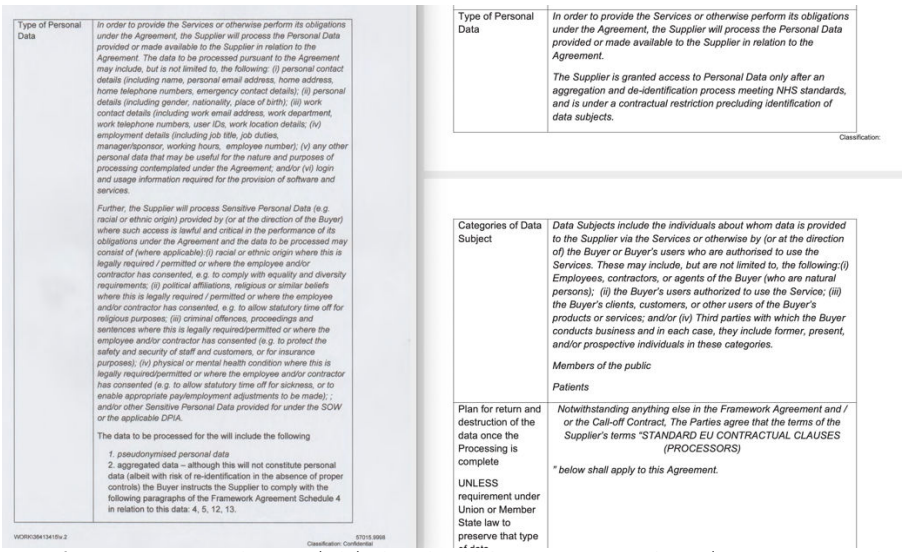
Though the NHS has not confirmed the extent of the types of personal data that Palantir accessed – the extension contract features significant changes in the types of personal data made available to Palantir. The initial contract provided that Palantir would reasonably have access to various types of personal data, including personal contact details; personal details; work contact and employment details; "any other personal data that may be useful"; and where necessary, race/ethnicity info, political affiliations, criminal history, and

[34] Palantir, IPO Investment Prospectus, 17 September 2020, p 95 https://www.sec.gov/Archives/edgar/data/1321655/000119312520248369/d904406ds1a.htm#rom904406_14

[35] PI and others, "(Sort of) Trust but Verify: Palantir Responds to Questions about its work with NHS", 6 May 2020, https://privacyinternational.org/long-read/3751/sort-trust-verify-palantir-responds-questions-about-its-work-nhs.

[36] Williams, O., "Revealed: Palantir secures £1m contract extension for NHS data store work", *NS Tech*, 15 July 2020, https://tech.newstatesman.com/coronavirus/palantir-nhs-datastore-contract-extension.

physical/mental health condition.[37] In the newer contract, they have removed the level of detail and the contract just uses standard definition of personal data.[38] See the 'type of personal data' box in the respective contracts below.



Type of Personal Data	*In order to provide the Services or otherwise perform its obligations under the Agreement, the Supplier will process the Personal Data provided or made available to the Supplier in relation to the Agreement. The data to be processed pursuant to the Agreement may include, but is not limited to, the following: (i) personal contact details (including name, personal email address, home address, home telephone numbers, emergency contact details); (ii) personal details (including gender, nationality, place of birth); (iii) work contact details (including work email address, work department, work telephone numbers, user IDs, work location details; (iv) employment details (including job title, job duties, manager/sponsor, working hours, employee number); (v) any other personal data that may be useful for the nature and purposes of processing contemplated under the Agreement; and/or (vi) login and usage information required for the provision of software and services.* *Further, the Supplier will process Sensitive Personal Data (e.g. racial or ethnic origin) provided by (or at the direction of the Buyer) where such access is lawful and critical in the performance of its obligations under the Agreement and the data to be processed may consist of (where applicable):(i) racial or ethnic origin where this is legally required / permitted or where the employee and/or contractor has consented, e.g. to comply with equality and diversity requirements; (ii) political affiliations, religious or similar beliefs where this is legally required / permitted or where the employee and/or contractor has consented, e.g. to allow statutory time off for religious purposes; (iii) criminal offences, proceedings and sentences where this is legally required/permitted or where the employee and/or contractor has consented (e.g. to protect the safety and security of staff and customers, or for insurance purposes); (iv) physical or mental health condition where this is legally required/permitted or where the employee and/or contractor has consented (e.g. to allow statutory time off for sickness, or to enable appropriate pay/employment adjustments to be made); ; and/or other Sensitive Personal Data provided for under the SOW or the applicable DPIA.* *The data to be processed for the will include the following* *1. pseudonymised personal data* *2. aggregated data – although this will not constitute personal data (albeit with risk of re-identification in the absence of proper controls) the Buyer instructs the Supplier to comply with the following paragraphs of the Framework Agreement Schedule 4 in relation to this data: 4, 5, 12, 13.*

Type of Personal Data	*In order to provide the Services or otherwise perform its obligations under the Agreement, the Supplier will process the Personal Data provided or made available to the Supplier in relation to the Agreement.* *The Supplier is granted access to Personal Data only after an aggregation and de-identification process meeting NHS standards, and is under a contractual restriction precluding identification of data subjects.*

Categories of Data Subject	*Data Subjects include the individuals about whom data is provided to the Supplier via the Services or otherwise by (or at the direction of) the Buyer or Buyer's users who are authorised to use the Services. These may include, but are not limited to, the following:(i) Employees, contractors, or agents of the Buyer (who are natural persons); (ii) the Buyer's users authorized to use the Service; (iii) the Buyer's clients, customers, or other users of the Buyer's products or services; and/or (iv) Third parties with which the Buyer conducts business and in each case, they include former, present, and/or prospective individuals in these categories.* *Members of the public* *Patients*
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type	*Notwithstanding anything else in the Framework Agreement and / or the Call-off Contract, The Parties agree that the terms of the Supplier's terms "STANDARD EU CONTRACTUAL CLAUSES (PROCESSORS)* *" below shall apply to this Agreement.*

Screenshots of contracts made available by the UK government. Initial contract on the left.

If tendering is designed to get the best value for a government, then surely there can be no better value than £1 – which is what the initial NHS contract was awarded for[39]. This initial offer – at a loss to themselves – may appear to be exceedingly cheap. However, there have been concerns raised about customers being unable to easily move their data off of Palantir's platform – tying them in for the long run and making Palantir a great deal of money. When the New York Police Department (NYPD) tried to cancel its contract with Palantir and requested copies of the analyses of their data, Palantir reportedly refused to provide them in a standardised format that the NYPD would be able to use with their next system.[40]

[37] Palantir initial contract as released by the government, now available here https://notechfortyrants.org/wp-content/uploads/2020/06/Palantir_Agreements.pdf.
[38] New contract between NHS and Palantir, released 26 August 2020, available here https://www.contractsfinder.service.gov.uk/Notice/c66036ee-a63e-4452-bafe-2410e9b51587?origin=SearchResults&p=1.
[39] No Tech For Tyrants, "The Corona Contracts", 7 June 2020, https://notechfortyrants.org/2020/06/07/the-corona-contracts/.
[40] Alden, W., "There's A Fight Brewing Between the NYPD and Silicon Valley's Palantir", *Buzzfeed* 28 June 2018, https://www.buzzfeednews.com/article/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley#.vamWb8V6G1.

Palantir's business plan raises questions about whether current Government tendering processes have the sophistication to deal with this sort of offer.

Transparency in public private partnerships ensures that the entire agreement is scrutinised to ensure that there are not any hidden clauses or benefits for the contracting company.

On top of the revenue guaranteed by the extended contract, based on the part of the contract that has been made available[41], NHS will not be the intellectual property owner of the product developed for the NHS datastore projects. Only following a legal challenge initiated by civil society, were the contracts reportedly released[42], clause 11.2[43] of the disclosed contract stipulates that

> "The Supplier [Palantir] grants the Buyer [NHS] a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities."

This means that Palantir retains intellectual property rights in the products it specifically develops for the NHS, while also licensing those rights to them. Beyond the monetary compensation for the licensing of Palantir's product, Foundry, Palantir stands to gain further insight and the ability to improve Foundry based on the NHS deployment.

The NHS has released Data Protection Impact Assessments with both the original and the extended contracts. Upon the publication of the extended contract, the NHS also published a Risk Assessment document that showed evaluation of various privacy concerns and risks.[44] However, the types of

[41] Fitzgerald, M., Crider C., "Under pressure, UK government releases NHS COVID data deals with big tech", *Open Democracy*, 5 June 2020, https://www.opendemocracy.net/en/under-pressure-uk-government-releases-nhs-covid-data-deals-big-tech/.
[42] *Ibid.*
[43] New contract between NHS and Palantir, released 26 August 2020, available here https://www.contractsfinder.service.gov.uk/Notice/c66036ee-a63e-4452-bafe-2410e9b51587?origin=SearchResults&p=1.
[44] NHS England, "Data Protection Impact Assessment: NHS COVID-19 Data Store", 15 June 2020, https://www.england.nhs.uk/publication/data-protection-impact-assessment-nhs-covid-19-data-store/.

potential risks identified via the categorisation on the risk assessment do not exhaust the full scope of risks of working with Palantir. For example, the "risk of re-identification for analysts who have access to pseudonymised record level data" is allegedly mitigated by strict protocols for accessing pseudonymised records, and appropriate training and contracting for employees.

Improvement clauses

In the rare Palantir contracts we could find in various answers to freedom of information requests (FOI requests), we observed that Palantir is routinely making use of "improvement" clauses. For instance, in a 2019 license agreement with the US Department of Defence (DoD), the company's terms and conditions document contained the following clause with regards to usage data:

> *"10. Usage Data. Palantir may collect analytics, statistics, metrics, or other usage data related to Customer's use of the Products (i) in order to provide the Products to Customer; (ii) for statistical use (provided that such data is not personally identifiable); or (iii) to monitor, analyze, maintain and improve the Products"* (emphasis added).[44]

The same document defines products as *"the Client Software, Cloud Solutions and Software specified in the Order"*[45] and software as *"the Palantir proprietary commercial software, models, and algorithms, and any helpers, extensions, plug-ins and add-ons, in any format, specified in the Order (…)"* (emphasis added).[46] Therefore, this clause enables Palantir to improve its algorithms or systems based on its customers' use of the Palantir products. In this specific case, the DoD acquired licenses for both Gotham and Metropolis[47] but Palantir has made use of such type of clauses in other contracts as well.

On the product pages of Gotham and Foundry found on the UK Government Digital Marketplace, we found out that both products reply to the exact same licensing terms and conditions, which contain the following clause:

> *"18.9. Usage Data. Palantir may collect metrics, analytics, statistics or other data related to Customer's use of the Cloud Solutions (i) in order to provide the Cloud Solutions, Support Services and Professional Services to and for the benefit of the Customer ; and (ii) for statistical use as well as to analyze, maintain and improve the Cloud Solutions, Support Services and Professional Services (provided that it makes such data not personally identifiable."* (emphasis added).[48]

While the typographical error contained in the last sentence eloquently shows that this part of the clause may have been hastily integrated for European customers, the clause is extremely similar to that of the DoD contract above.[49]

Thus, it appears that through these "improvement" clauses, Palantir reserves itself the right to improve its systems, including those of Gotham and Foundry and irrespective of whether these tools are sold as a combined solution or separately.

POLICING (LONDON MET, DURHAM, GREATER MANCHESTER & SOMERSET)

Predictive policing has increasingly been touted as the next frontier in tech-enhanced policing, and has been[51] embraced in the United States. Palantir's services, including its signature Gotham platform, have been utilised by police forces across America and these agreements are reportedly sometimes established through backroom deals.[52]

Though UK constabularies have been slower to introduce the use of predictive policing capabilities, we know from Liberty's Freedom of Information requests regarding predictive policing in the UK[53] that several UK constabularies have

[45] See FOIA Online, 'DON-NAVY-2009-009066 Request Details – BPA Attachment 3 – DoD License Agreement; Palantir Terms and Conditions', 21 August 2019, https://www.foiaonline.gov/foiaonline/action/public/submissionDetails?trackingNumber=DON-NAVY-2019-009066&type=request accessed 23 April 2020.
[46] Ibid.
[47] Ibid.
[48] Metropolis is the solution that predates Foundry and is used predominently in the financial services industry.
[49] See Gov.uk Digital Marketplace – Palantir Gotham 'Palantir Licensing Terms and Conditions', https://assets.digitalmarketplace.service.gov.uk/g-cloud-11/documents/92736/660200105725744-terms-and-conditions-2019-05-22-1447.pdf together with Gov.uk Digital Marketplace – Palantir Foundry 'Palantir Licensing Terms and Conditions' https://assets.digitalmarketplace.service.gov.uk/g-cloud-11/documents/92736/501000199851013-terms-and-conditions-2019-05-22-1449.pdf. Cloud Solution is described in Palantir's licencing terms and conditions as follow: "1.5. "Cloud Solution(s)" means Palantir's service to provide a cloud software platform for data analysis, including access to proprietary Palantir software as specified in the Order, software provided to Customer in connection with this Agreement, and any Cloud Updates that are made available in connection with this Agreement (and/or in connection with any future or related Orders, or amendments).
[50] NHS England, "Data Protection Impact Assessment: NHS COVID-19 Data Store", 15 June 2020, https://www.england.nhs.uk/publication/data-protection-impact-assessment-nhs-covid-19-data-store/.
[51] Lau, T., "Predictive Policing Explained", Brennan Center for Justice, 1 April 2020, https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained Ahmed M., "Aided by Palantir, the LAPD Uses Predictive Policing to Monitor Specific People and Neighborhoods", The Intercept, 11 May 2018, https://theintercept.com/2018/05/11/predictive-policing-surveillance-los-angeles/
[52] Winston, A., "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.
[53] Couchman, H., "Policing by Machine: Predictive policing and the threat to our rights", Liberty, January 2019, https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/LIB-11-Predictive-Policing-Report-WEB.pdf

already trialled, or are in the process of trialling, various predictive policing technologies. For example, in Avon & Somerset, police used predictive mapping along with an alarmingly broad variety of individual risk assessment programs.[54] Additionally, Durham constabulary partnered with the Department of Criminology at the University of Cambridge to create an individual risk assessment program (HART).[55]

As predictive policing gains traction amongst UK police constabularies, Palantir's name starts appearing as a supplier of such technology. Indeed, the same report by Liberty revealed that the London Met had trialled Palantir Predictive Crime Mapping products for a period of twelve months, from May 2014 to April 2015.[56] It is not known what product the London Met trialled, nor how the data was processed or shared with Palantir.

It is not known if London Met has other contracts with Palantir. However, various reports indicate that Palantir has continued to have connections with the London Met. The Met's Chief attending a reception hosted by London First (a business group) at Palantir's Soho office in July 2018.[57] Just over a year later, Palantir sponsored £3,000 of reception drinks in exchange for a promotional stand at a counter terrorism border conference.[58] In December 2019, Palantir sponsored a drinks reception that Lancashire assistant chief constable Tim Jacques attended[59]. Police should have to disclose their participation in such private events, as they represent an obvious attempt to secure business.

---

[54] Ibid.
[55] *Ibid.*
[56] Couchman, H., "Policing by Machine: Predictive policing and the threat to our rights", *Liberty,* January 2019, https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/LIB-11-Predictive-Policing-Report-WEB.pdf.
[57] National Crime Agency, Board Member, Gifts & Hospitality Register 2018/19, 1 April – 21 March 2019, https://nationalcrimeagency.gov.uk/who-we-are/publications/318-gifts-hospitality-nina-cope-2018-19-2/file%20l"
[58] Metropolitan Police, Freedom of Information Act Publication Scheme, 1 October 2019, https://www.met.police.uk/SysSiteAssets/foi-media/metropolitan-police/priorities_and_how_we_are_doing/corporate/commercial--finance---section-93-agreements-under--10k-q3---20192020.
[59] Metropolitan Police, Freedom of Information Act Publication Scheme, March 2020, https://www.met.police.uk/SysSiteAssets/foi-media/metropolitan-police/lists_and_registers/corporate/professionalism---management-board---gifts-and-hospitality-register---december-2019.

In seeking clarity over the Met's engagements with Palantir, No Tech filed a Freedom of Information request on 15 June 2020 seeking information regarding the Metropolitan Police Service's (MPS) May 2014 - April 2015 trial of Palantir Software.[60] We sought more information on the types of data processed by the Palantir products being trialled between May 2014 - April 2015, and whether the MPS was currently testing, piloting, or using any products or services developed by Palantir since 2018. At the time of writing there has been no response from the MPS – far overdue given the legal requirement to respond to such requests within 20 working days.

MINISTRY OF DEFENCE

The UK Ministry of Defence (MoD) reportedly has at least £28m worth of deals with Palantir, as of December 2019. There is limited transparency about what the contracts involve.

What is known so far is that they include a 2018 contract, with a value of £1.7m, to use Palantir software for the purpose of slowing down the rate of staff voluntarily leaving the Navy. The software was used for "personnel data manipulation to discover reasons for voluntary outflow rates and enable the [Royal Navy] to develop possible solutions." [61] In late 2019, Palantir also secured a deal with the MoD for the "provision and support of a search visualisation and analysis system," [62] though it is not known for what Palantir product.

[60] No Tech for Tyrants, "Palantir Technologies products used by MPS FOI Request", date submitted 15 June, https://www.whatdotheyknow.com/request/palantir_technologies_products_u_4.
[61] Williams, O., "How Peter Thiel's Palantir quietly won £10m of MoD contracts", *News Statesman,* 6 August 2019, https://www.newstatesman.com/politics/business-and-finance/2019/08/how-peter-thiel-s-palantir-quietly-won-10m-mod-contracts".
[62] Williams, O., "Peter Thiel's Palantir has quietly secured £39m of UK government deals", NS Tech, 3 December 2019, https://tech.newstatesman.com/cloud/peter-thiel-palantir-mod-contracts-2.

Ministry of Defence Response

On 21st September 2020, the MoD responded to our FOI request confirming that they are currently using Foundry, and that they have a contract with Palantir but did not disclose the contract with their response. They also clarified that Palantir is acting as a processor for non-personal data.

However, they didn't provide an answer to our question regarding personal data. Invoking exemptions, such as safeguarding national security, they neither confirmed nor denied if the company process personal data or what categories of personal data they process if they do.

The MoD claim that:

> "The environment hosting the personal information is located within the MoD data boundary. There is no mechanism to take the data out of this environment. On analysis, the data is anonymised. Personnel with access are security cleared accordingly. There are limits on the number of personnel permitted access and access to the system is governed by several layers of permission. Logs of access to data are retained and scrutinised for improper use."

However, it is unclear exactly what this means in the context of how Palantir normally operates. Palantir's technology is cloud based and is normally supplied via Amazon Web Services (see NHS contract). It is unclear if the MOD's environment is hosted externally.

It is also unclear what staff at Palantir would have access to. The MoD's response focuses solely on MoD personnel.

The MoD has also not released the Data Protection Impact Assessment that could have cleared up some of these concerns.

A Freedom of Information request was sent to the MoD in May 2020[63] by No Tech For Tyrants about which Palantir products it is currently testing, piloting, or using. The MoD delayed their response to consider possible reasons for withholding the information, namely, for protecting "National Security" and "Commercial Interests."

[63] Ministry of Defence response to No Tech For Tyrants Freedom of Information Request, 24 June 2020, https://www.whatdotheyknow.com/request/667332/response/1590853/attach/3/FOI2020%2006109%20Moore%20Interim%20Response%201.pdf?cookie_passthrough=1" \h.

They neither confirmed nor denied that they hold any more information in addition to the information provided in the Annex dated 17 August 2020.[64]

Another product the MoD may be reportedly testing is Palantir's Defence Intelligence Platform. Palantir is an approved government Digital Marketplace vendor in the United Kingdom, and the Defence Intelligence Platform is one of the products available for sale.[65] The platform "enables defence intelligence agencies to integrate disparate data sources into unified investigations for counterterrorism and intelligence workflows. The platform facilitates shared situational awareness, analysis and defence collaboration, while securing data against unauthorised access."[66] Not only is it not fully known to the public what products and software are being used, it is also not known what kinds of data, including personal data, are being processed by products like this.

CABINET OFFICE

The Cabinet Office, the UK department responsible for supporting the UK Prime Minister and Cabinet, has reportedly spent at least £1,417,834 contracting with Palantir. Specifically, £741,000 of this amount was reportedly spent for IT services provided by Palantir Technologies[67] - the nature of this "enterprise analytical platform and intelligence service" has not been publicly disclosed. The remaining reported £1.4 million was for cloud services[68] from Palantir which also have not been disclosed in detail.

[64] 'Palantir Technologies products used by the Ministry of Defence' FOI: https://www.whatdotheyknow.com/request/palantir_technologies_products_u_2
[65] Palantir Defence Intelligence Platform, UK Gov Digital Marketplace: https://www.digitalmarketplace.service.gov.uk/g-cloud/services/246057090713388.
[66] *Ibid*.
[67] Murphy, M, "Peter Thiel's 'invasive' Palantir on push to ramp up secretive UK government contracts", *The Telegraph,* 9 December 2018, https://www.telegraph.co.uk/technology/2018/12/09/peter-thiels-invasive-palantir-push-ramp-secretive-uk-government/.
[68] Advicecloud, Analyse G-Cloud sales, https://advice-cloud.co.uk/spend-data/gcloud-sales/.

Despite the considerable sums the Cabinet Office has spent on Palantir products, the government has been reticent to provide information regarding which entity controls the data. No Tech For Tyrants has tried to gain greater insights into these contracts by submitting a Freedom of Information request seeking information on the Cabinet Office's use of Palantir products[69]: the kind of data processed by said products; the control of this data; and whether a Data Impact Assessment or Equality and Human Rights Impact Assessment was undertaken. The prevalent use of non-disclosure agreements[70] in Palantir's contracts is especially concerning given the extent of their contracts with the Cabinet Office.

The failure of the Cabinet Office to provide further detail on its contracts with Palantir leaves crucial questions of data security and protection unanswered – leaving the public unaware of how their data is shared and processed.

In the face of the government's silence regarding its existing and prior contracts with Palantir, the recent news that the government has awarded Palantir 'oversight of the UK's post-Brexit border and customs data'[71] is cause for alarm. The Guardian reported [72] that the contract gives Palantir management of the data analytics and architecture of the 'new "border flow tool", which will collate data on the transit of goods and customs.' Privacy International has requested further information and clarifications from the Cabinet Office with regard to these new reported agreements. At the moment of writing we are waiting for their response.

With such a significant contract on the horizon, it is the responsibility of the Cabinet Office to disclose more information about past and current contracts with Palantir.

[69] No Tech For Tyrants Freedom of Information request to the Cabinet Office: https://www.whatdotheyknow.com/request/palantir_technologies_products_u.
[70] https://www.businessinsider.com/palantir-ice-explainer-data-startup-2019-7?r=US&IR=T
[71] Pegg, D., "UK awards border contract to firm criticised over role in US deportations", *The Guardian,* 17 September 2020, https://www.theguardian.com/politics/2020/sep/17/uk-awards-border-contract-to-firm-criticised-over-role-in-us-deportations?CMP=Share_iOSApp_Other.
[72] *Ibid.,*

ENTRENCHING INJUSTICE?

Given Palantir's reported track record of digital profiling and collaborating with ICE to facilitate the deportation of undocumented workers[73], there is a vast range of data that, if being processed by Palantir in the UK, is cause for concern. This could be personal data: nationality, information contained in asylum applications, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, a person's sex life or sexual orientation, and data revealing criminal convictions or offences. With Palantir's NHS contract, there is increasing risk of access to a person's genetic data, biometric data, and data concerning health.

Datafication is not always an 'objective' way of finding solutions to social problems. In fact, often the use of data in particular ways can entrench existing inequities and lead to pre-determined 'solutions.' An example of this in the UK is the Border Agency's Human Provenance Pilot (HPP) Project[74], which aimed to "use DNA and isotope analysis of tissue from asylum seekers to evaluate their nationality and help decide who can enter the United Kingdom."[75] Aside from glaring ethical issues with the proposal, scientific experts widely decried the fallacy that DNA could pinpoint ethnic or national origins.[76] With no scientific basis for what the data was made to mean, the data produced by the project risked making an already cruel and exhausting process even more so by adding an additional arbitrary barrier.

Palantir's growing role in a range of UK government bodies, coupled with the lack of transparency from the government on what this role entails, means Palantir will have increasing access to data about people living in the UK, and the power to shape the processing and analysis of this data, with no accountability to the public.

---

[73] MacMillan D. and Dwoskin E., "The war inside Palantir: Data-mining firm's ties to ICE under attack by employees", *Washington Post,* 22 August 2019, https://www.washingtonpost.com/business/2019/08/22/war-inside-palantir-data-mining-firms-ties-ice-under-attack-by-employees/.

[74] *BBC News*, "Experts condemn asylum DNA tests", 30 September 2019, http://news.bbc.co.uk/1/hi/uk/8282654.stm.
[75] Travis, J., " Scientists Decry Isotope, DNA Testing of 'Nationality'", *Science,* 2 October 2009, https://science.sciencemag.org/content/326/5949/30.summary.
[76] *BBC News*, "Experts condemn asylum DNA tests", 30 September 2019, http://news.bbc.co.uk/1/hi/uk/8282654.stm.

There is no transparency around which Palantir products the UK government bodies use in many cases; nor do we know if Data Protection Impact Assessments and Equality and Human Rights Impact Assessments are completed in relation to all Palantir products deployed. And one of the problems with a private company holding or even just having access to so much information about the public is that requests for transparency can be denied as a matter of protecting 'commercial interest.'

In other words, we often do not know what, if any, safeguards are in place to protect our data, and ensure that it is not misused – for discriminatory policing, for unjustified deportation of those already living precariously in the UK, for training new technology in a way that could replicate these kinds of abuses.

The extent to which Palantir is already involved in the functioning of the UK government should be alarming for those concerned with transparency and accountability. As we have written previously,

> "when states transfer more power to private entities, the public loses. The government becomes a body designed to service the needs and interests of profit-seeking private entities rather than its citizens. Worse, citizens lose much of their power to hold governments accountable: the government abdicates and transfers responsibility to private actors against which citizens have fewer rights."[77]

[77] Privacy International and No Tech For Tyrants, "*The Corona Contracts: Public-Private Partnerships and the Need for Transparency*", 26 June 2020, http://privacyinternational.org/long-read/3977/corona-contracts-public-private-partnerships-and-need-transparency.

PALANTIR'S GLOBAL RECORD

A closer look at Palantir's engagements on a global scale highlights that the company provides services around the world, often with a similar lack of transparency.

PALANTIR IN THE US

It's hard to overstate Palantir's close relationship with the US government. The data analysis company has contracts with, among others, the Department of Defense[78], Department of Justice[79], Department of Health and Human Services[80], the Securities and Exchange Commission[81], the Department of State[82], the Department of Agriculture[83], the Department of Commerce[84], and the Department of Homeland Security[85]. Through its venture capital branch In-Q-Tel, the US Central Intelligence

[78] US Government contracts with the Department of Defense: https://www.fpds.gov/ezsearch/fpdsportal?q=palantir+DEPARTMENT_FULL_NAME%3A%22DEPT+OF+DEFENSE%22&s=FPDSNG.COM&templateName=1.5.1&indexName=awardfull&x=0&y=0&sortBy=SIGNED_DATE&desc=Y.
[79] US Government contracts with the Department of Justice: https://www.fpds.gov/ezsearch/fpdsportal?q=palantir+DEPARTMENT_FULL_NAME%3A%22JUSTICE%2C+DEPARTMENT+OF%22&s=FPDSNG.COM&templateName=1.5.1&indexName=awardfull&x=0&y=0.
[80] US Government contracts with the Department of Health and Human Services: https://www.fpds.gov/ezsearch/fpdsportal?q=palantir+DEPARTMENT_FULL_NAME%3A%22HEALTH+AND+HUMAN+SERVICES%2C+DEPARTMENT+OF%22&s=FPDSNG.COM&templateName=1.5.1&indexName=awardfull&x=0&y=0.
[81] US Government contracts with the Securities and Exchange Commission: https://www.fpds.gov/ezsearch/fpdsportal?q=palantir+DEPARTMENT_FULL_NAME%3A%22SECURITIES+AND+EXCHANGE+COMMISSION%22&s=FPDSNG.COM&templateName=1.5.1&indexName=awardfull&x=0&y=0.
[82] US Government contracts with the Department of State: https://www.fpds.gov/ezsearch/fpdsportal?q=palantir+DEPARTMENT_FULL_NAME%3A%22STATE%2C+DEPARTMENT+OF%22&s=FPDSNG.COM&templateName=1.5.1&indexName=awardfull&x=0&y=0.
[83] US Government contracts with the Department of Agriculture: https://www.fpds.gov/ezsearch/fpdsportal?q=palantir+DEPARTMENT_FULL_NAME%3A%22AGRICULTURE%2C+DEPARTMENT+OF%22&s=FPDSNG.COM&templateName=1.5.1&indexName=awardfull&x=0&y=0.
[84] US Government contracts with the Department of Commerce: https://www.fpds.gov/ezsearch/fpdsportal?q=palantir+DEPARTMENT_FULL_NAME%3A%22COMMERCE%2C+DEPARTMENT+OF%22&s=FPDSNG.COM&templateName=1.5.1&indexName=awardfull&x=0&y=0.
[85] US Government contracts with the Department of Homeland Security: https://www.fpds.gov/ezsearch/fpdsportal?q=palantir+DEPARTMENT_FULL_NAME%3A%22HOMELAND+SECURITY%2C+DEPARTMENT+OF%22&s=FPDSNG.COM&templateName=1.5.1&indexName=awardfull&x=0&y=0.

Agency invested in Palantir as a start-up.[86] According to a 2019 report by the US-based advocacy organization Mijente, the CIA also provided creative direction for Palantir's forays into counter-terrorism, and is still a shareholder in Palantir.[87]

Palantir and the U.S. Department of Health and Human Services

Palantir has played an integral role in the US effort to process and analyse data related to Covid-19. On April 10, U.S. Department of Health and Human Services (HHS) awarded Palantir a $17.4 million contract with a subsidiary agency, the Program Support Center (PSC).[88] The money, which came out of the federal government's Covid-19 relief fund, is being used to license Gotham.

And on April 21, it was reported that Palantir was granted additional funds ($7.5 million) to help with the HHS Protect platform, which "...pulls data from across the federal government, state and local governments, healthcare facilities, and colleges, to help administration officials determine how to 'mitigate and prevent spread' of the coronavirus."[89]

The Palantir contracts worried Congressional Hispanic Caucus (CHC) members. They were concerned "...about the use of this health data for purposes beyond the preservation of public health."[90] In the past, the Trump administration has permitted Immigration and Customs Enforcement (ICE) to access confidential data collected by the HHS. The Brennan Center for Justice notes that historical collaboration

[86] Waldman, P. and others, "Peter Thiel's data-mining company is using War on Terror tools to track American citizens. The scary thing? Palantir is desperate for new customers.", *Bloomberg*, 19 April 2018, https://www.bloomberg.com/features/2018-palantir-peter-thiel/; Brewster T., "Palantir, The Peter Thiel-Backed $20 Billion Big Data Cruncher, Scores $17 Million Coronavirus Emergency Relief Deal", *Forbes*, 21 April 2020, https://www.forbes.com/sites/thomasbrewster/2020/04/11/palantir-the-peter-thiel-backed-20-billion-big-data-cruncher-scores-17-million-coronavirus-emergency-relief-deal/#4e03b4c95ed1.

[87] Mijente, "The War Against Immigrants: Trump's Tech Tools Powered By Palantir", 2019 https://notechforice.com/palantir/, pp 28-29.

[88] *Contract Summary – Delivery Order (DO) PIID 75P00120F80084.* (n.d.). Retrieved 16 September 2020 from https://www.usaspending.gov/award/CONT_AWD_75P00120F80084_7570_GS35F0086U_4730 .

[89] Brewster T., "Palantir, The Peter Thiel-Backed $20 Billion Big Data Cruncher, Scores $17 Million Coronavirus Emergency Relief Deal", *Forbes*, 21 April 2020, https://www.forbes.com/sites/thomasbrewster/2020/04/11/palantir-the-peter-thiel-backed-20-billion-big-data-cruncher-scores-17-million-coronavirus-emergency-relief-deal/#4e03b4c95ed1.

[90] Congressional Hispanic Caucus Members, "*Press Release: Congressional Hispanic Caucus Members Demand Trump Administration Release HHS Contracts with Palantir",* 25 June 2020, https://chc.house.gov/media-center/press-releases/congressional-hispanic-caucus-members-demand-trump-administration.

between HHS and ICE has led directly to the arrest and deportation of hundreds of immigrants.[91] An HHS spokesperson rejected the CHC's concerns, but Democratic senators were unsatisfied with the response.[92] Given Palantir's work with ICE and HHS's prior collaboration, the senators worried that "...data in HHS Protect could be used by other federal agencies in unexpected, unregulated, and potentially harmful ways, such as in the law and immigration enforcement context."[93]

The senators' worries were amplified when HHS took over control of COVID-19 reporting by hospitals from the Centers for Disease Control and Prevention (CDC) in mid-July.[94] Though the CDC re-gained responsibility for data collection in late August, concerns remain.[95]

Palantir and the U.S. Department of Homeland Security

As mentioned already, Palantir has faced significant public criticism for its contracts with US Immigration and Customs Enforcement (ICE), an agency under the US Department of Homeland Security (DHS), who have faced significant outcry over their policy of separating children from their families, and keeping them in horrific conditions.[96] In their response Palantir clarified that they do not hold contracts with the Enforcement and Removal Operations (ERO) division of ICE or U.S. Customs and Border Protection (CBP).[97]

---

[91] Brennan Center for Justice, *Resource: DHS-HHS Information Sharing and ICE Enforcement Against Potential Sponsors of Detained Children: A Resource Page*, 6 December 2018, https://www.brennancenter.org/our-work/research-reports/dhs-hhs-information-sharing-and-ice-enforcement-against-potential.

[92] Glaser, A., "Latino House Democrats demand answers on government coronavirus contracts with Palantir", *NBC News*, 25 June 2020, https://www.nbcnews.com/tech/tech-news/latino-house-democrats-demand-answers-government-coronavirus-contracts-palantir-n1232156.

[93] "Letter to HHS from Democratic senators and members of Congress on HHS Protect Now incentive", *The Washington Post*, 1 July 2020, https://www.washingtonpost.com/context/context-card/e33ec35b-9455-4da1-a035-815d195fb65c/?itid=lk_inline_manual_5.

[94] Redfield, R., "Prepared Remarks from HHS Media Call with CDC Director Redfield and CIO Arrieta on COVID-19 Data Collection, *HHS.gov.*, 15 July 2020, https://www.hhs.gov/about/news/2020/07/15/prepared-remarks-from-hhs-media-call-cdc-director-redfield-cio-arrieta-covid-19-data-collection.html.

[95] Whelan, R., "Covid-19 Data Will Once Again Be Collected by CDC, in Policy Reversal", *The Wall Street Journal*, 20 August 2020, https://www.wsj.com/articles/troubled-covid-19-data-system-returning-to-cdc-11597945770.

[96] Holpuch, A., "Trump's separation of families constitutes torture, doctors find", *The Guardian,* 25 February 2011, https://www.theguardian.com/us-news/2020/feb/25/trump-family-separations-children-torture-psychology.

[97] See full response of Palantir in Annex 1 of this report.

The company reportedly built and helped to deploy a data analysis platform used by US immigration authorities – called Investigative Case Management System.[98] The platform according to these reports allows agents to query multiple databases at one time, as opposed to agents being required to perform the same search across dozens or more databases. [99]

Palantir's case management tools are said to be "mission critical" to ICE[100]; and it has been reported that the Palantir tool FALCON played an instrumental role in the mass immigration raids of almost 700 people in Mississippi in August 2019.[101]

Though Palantir representatives tend to state that Palantir stays away from powering deportations in its work with the Department for Homeland Security, Mijente, a US activist group, has alleged that FALCON and the investigative case management tools provided by Palantir are specifically used by ICE for raids and tracking, respectively.[102] The American Civil Liberties Union (ACLU) claimed that the investigative case management system "ingests commercial license plate reader (LPR) data shared by local law enforcement in at least 80 jurisdictions across the country, violating local law and ICE policy."[103]

Palantir and Project Maven

Project Maven, created in 2017, is a US Department of Defence artificial intelligence

---

[98] Woodman, Sp., "Palantir Provides the Engine for Donald Trump's Deportation Machine", *The Intercept*, 2 March 2017, https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/.
[99] *Ibid.*
[100] Mijente, "The War Against Immigrants: Trump's Tech Tools Powered By Palantir", 2019 https://notechforice.com/palantir/, p 4.
[101] Joseph, G., "Data Company Directly Powers Immigration Raids in Workplace | WNYC | New York Public Radio, Podcasts", *Live Streaming Radio, News*, WNYC, 16 July 2019, https://www.wnyc.org/story/palantir-directly-powers-ice-workplace-raids-emails-show/; Mijente, "BREAKING: Palantir's technology used in Mississippi raids where 680 were arrested | #NoTechForICE", 4 October 2015, https://notechforice.com/breaking-palantirs-technology-used-in-mississippi-raids-where-680-were-arrested/.
[102] Mijente, "The War Against Immigrants: Trump's Tech Tools Powered By Palantir", 2019 https://notechforice.com/palantir/, p 10.
[103] Quote from Mijente, "The War Against Immigrants: Trump's Tech Tools Powered By Palantir", 2019 https://notechforice.com/palantir/, p. 8. But see also, Talla, V. "Documents Reveal ICE Using Driver Location Data From Local Police for Deportations", ACLU, 13 March 2019, https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data.

drone project that was originally contracted to Google. After protests from employees, Google announced in 2018 that it would be walking away from the Maven contract.[104] In December 2019, news broke that the contract would be awarded to Palantir.[105]

Previously named the Algorithmic Warfare Cross-Functional Team, Project Maven uses artificial intelligence to do imaging analysis on drone footage (for example, by identifying and tagging different types of objects that appear in the footage) and ultimately attempts to improve the Pentagon's drone usage capabilities.

PALANTIR IN EUROPE

In July 2019, the Gesellschaft für Freiheitsrechte in Germany, filed legal proceedings with Karlsruhe Constitutional Court against Hessen Police for the expansion of surveillance powers, obtained through their contract with Palantir.[106] The Palantir-supplied policing software suite, known as Hessendata, reportedly triangulates a number of distinct datasets from police and other databases, including social media, enabling the analysis of potential suspects.[107]

Palantir has also operated extensively in the neighbouring country, Denmark. In February 2017, following the 2016 purchase of software from Palantir Technologies, the Danish Ministry of Justice presented a draft legislation for public consultation with the objective of justifying the processing of personal data through the Palantir-supplied software (which exists in two iteration: POL-INTEL, for the Danish Police, and PET-INTEL, for the Danish Intelligence Service).[108] Circumventing the EU

[104] Greene, T., "Report: Google to abandon Project Maven after government contract ends", The Next Web, 1 June 2018, https://thenextweb.com/artificial-intelligence/2018/06/01/google-announces-it-wont-renew-military-ai-contract/.
[105] Greene, T., "Report: Palantir took over Project Maven, the military AI program too unethical for Google ", *The Next Web*, 11 December 2019, https://thenextweb.com/artificial-intelligence/2019/12/11/report-palantir-took-over-project-maven-the-military-ai-program-too-unethical-for-google/.
[106] Mattes, A. L., "Hessentrojaner und Hessendata greifen Grundrechte an", Gesellschaft für Freiheitrechte, 2 July 2019, https://freiheitsrechte.org/pm-vb-hessen/
[107] *Ibid*
108 Dahllof St. and others, "EU states copy Israel's 'predictive policing'', EU Observer, 6 October 2017, https://euobserver.com/justice/139277

Law Enforcement Directive through a national exemption, the contract, which was signed for 84 months[109], gives the PET and the Police the ability to allegedly identify likely cases of terrorism before they occur.[110] It is currently unclear exactly what variables are used, how data is parsed, and when something might flag up as a potential threat.

In addition to Germany and Denmark, Palantir's reported European operations include:

- Palantir and the European Commission[111]
- Palantir in France [112]
- Palantir also partnered with Scuderia Ferrari in Italy [113]
- Norwegian-based Marlink acquired Palantir's Norway division[114]
- Palantir's partnership with Norwegian police and customs[115]

PALANTIR AND ISRAEL

The New York Times first reported in 2014 that Palantir has contracts with the Israeli government. Some employees protested those contracts, because they "…disagree

109 Winston, A., "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

110 This type of identification techniques is described by some as predictive policing. See our full answer to Palantir on point 10, Annex 2 to this report.

111 No Tech For Tyrants, "NoTechFor: (E)U", 14 July 2020, https://notechfortyrants.org/2020/07/14/notechfor-eu/

112 Cohen-Grillet, Ph., "Trump-linked US firm at heart of French intelligence", *EU Observer*, 9 June 2017, https://euobserver.com/beyond-brussels/138155.

113 *Palantir Foundry Enables Scuderia Ferrari Through Data", 4 September 2018, https://www.prnewswire.com/news-releases/palantir-foundry-enables-scuderia-ferrari-through-data-873451908.html.

114 Marlink acquires long-term vessel IT management partner Palantir, 17 March 2017, https://marlink.com/marlink-acquires-long-term-vessel-it-management-partner-palantir/.

115 Standal, B., "Storebrors synestein", *Dagbladet,* 4 April 2018, https://www.dagbladet.no/kultur/storebrors-synestein/69665007

with its [Israel's] policies toward Palestinians."[116] In 2017, Haaretz reported that Israeli security organisations contract with only two technology companies that provide predictive analytics systems: Fifth Dimension and Palantir.[117] Israel uses those systems to analyse social media posts for the purpose of identifying individuals who fit the "...terrorist profile."[118] As a consequence, Palestinians are reportedly surveilled, questioned, detained, and arrested for, say, "...posting photos of family members killed by Israeli forces or in prison, citing Quranic verses, or calling for protests."[119]

PALANTIR AND THE WORLD FOOD PROGRAMME

In February 2019, Palantir and the United Nations World Food Programme (WFP) entered a "five-year partnership aimed at helping WFP use its data to streamline the delivery of food and cash-based assistance"[120]. By bringing together a number of disparate complex datasets, Palantir's products (mainly 'Foundry') are allegedly enabling the UN mandated organisation to better meet the needs of vulnerable populations. However, a recent standoff between the WFP and Houthis in Yemen, who were denied aid in the face of refusal to register their biometric information, warrants proportionality concern over how far the institution will go to record invasive personal data on beneficiaries, even children.

This is further compounded by their Palantir contract, which enables the WFP to generate wide-scale insights, with the risk of seriously compromising the privacy of aid recipients, and in turn present Palantir with the opportunity to deploy, test, and improve their products on the back on fragile populations in contexts of suspended or limited rights. PI have questioned this partnership in the past, not least because

[116] Hardy, Q., "Unlock Secrets, if Not Its Own Value", *The New York Times*, 31 May 2014, https://www.nytimes.com/2014/06/01/business/unlocking-secrets-if-not-its-own-value.html.
[117] Hirschauge, O. and Shezaf H., "How Israel Jails Palestinians Because They Fit the 'Terrorist Profile.'", *Haaretz*, 31 May 2017, https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-jails-palestinians-who-fit-terrorist-profile-1.5477437.
[118] *Ibid.*
[119] *Ibid.*
[120] World Food Programme, "Palantir and WFP partner to help transform global humanitarian delivery", 5 February 2019, https://www.wfp.org/news/palantir-and-wfp-partner-help-transform-global-humanitarian-delivery.

of its potential violation of a principle of humanitarian action, namely that agencies are neutral.[121]

PALANTIR'S PRIVACY AND CIVIL LIBERTIES COUNCIL

In addition to its team of Privacy and Civil Liberties Engineers, Palantir has an advisory council of independent experts who provide insight related to privacy and digital civil liberties. In 2012, Palantir announced the creation of this body: the Palantir Council of Advisors on Privacy and Civil Liberties (PCAP)[122]. In 2014, PCAP expanded for a more European and international focus. PCAP members have included academics, digital civil liberties activists, and technology experts. Members are "free to criticize" Palantir's work, though they are under NDAs.[123]

Palantir says that:

> "particularly in the world of data analysis, liberty does not have to be sacrificed to enhance security. Palantir is constantly looking for ways to protect privacy and individual liberty through its technology while enabling the powerful analysis necessary to generate the actionable intelligence that our law enforcement and intelligence agencies need to fulfil their missions," and that at Palantir, "[w]e obligate ourselves to do what is right, not just what is legal."[124]

Such a statement gives the impression that Palantir is critically thinking about problems of right and wrong, of privacy and individual liberty – just behind closed doors. They claim they are working hard to create a better society that preserves

[121] PI, "One of the UN's largest aid programmes just signed a deal with the CIA-backed data monolith Palantir", 12 February 2019, http://privacyinternational.org/news-analysis/2712/one-uns-largest-aid-programmes-just-signed-deal-cia-backed-data-monolith.
[122] "Announcing the Palantir Council on Privacy and Civil Liberties", Palantir, November 2012, https://www.palantir.com/2012/11/announcing-the-palantir-council-on-privacy-and-civil-liberties/.
[123] Palantir. (n.d.), "Announcing the Palantir Council on Privacy and Civil Liberties. Palantir", Retrieved on 19 September 2020, from https://palantir.com/2012/11/announcing-the-palantir-council-on-privacy-and-civil-liberties.
[124] Palantir. (n.d.), "*Palantir Technologies—Privacy & Civil Liberties*. AU GradConnection". Retrieved 20 September 2020, from https://au.gradconnection.com/employers/palantir-technologies/privacy-civil-liberties/.

privacy and civil liberties and avoid mistaking algorithms for universal solutions to ethical problems. Palantir appears is conducting due diligence on paper. The next section highlights what needs to be done for this veneer of respect for privacy, liberty and civil rights to be verified and upheld in practice.

WHERE DO WE GO FROM HERE?

HOW DO WE HOLD THE UK GOVERNMENT AND PALANTIR TO ACCOUNT?

In the lead-up to the company's direct listing, we have witnessed an outburst of protest and concern across the US and UK, from migrants' rights activists to technologists to privacy scholars[125]. The message is clear: there is a global concern about such lack of transparency in public private partnerships. In order to ensure that Palantir does not continue to embed itself in the UK government without any scrutiny, continued public attention and engagement from all sectors is crucial. As more and more people develop concerns about the role of structurally problematic technologies in governance, it will be crucial to apply pressure to decision-makers who have always had the option of saying "no" to such agreements.

RECOMMENDATIONS FOR THE UK GOVERNMENT:

Against the backdrop of a crisis of confidence in the government's handling of data following the many scandals related to invasive practices around citizen data, (from Cambridge Analytica to the A-levels algorithm), it would behove the government to avoid yet another democratic deficit by introducing greater transparency and stricter protections on its dealings with tech giants. A number of actions can be carried out at this stage, especially in light of the increased momentum around Palantir's opening to markets.[126]

[125] Franco, M. "Palantir filed to go public. The firm's unethical technology should horrify us", The Guardian, 4 September 2020, https://www.theguardian.com/commentisfree/2020/sep/04/palantir-ipo-ice-immigration-trump-administration.
[126] Franco, M., "Palantir filed to go public. The firm's unethical technology should horrify us", *The Guardian,* 4 September 2020, https://www.theguardian.com/commentisfree/2020/sep/04/palantir-ipo-ice-immigration-trump-administration.

1) Incorporate human rights into public sector procurement policy

The government should ensure that all public sector procurement is conditioned upon the human rights compliance of the companies competing for the contracts. As underlined by the Parliamentary Committee on Human Rights, "If the Government expects businesses to take human rights issues in their supply chains seriously, it must demonstrate at least the same level of commitment in its own procurement supply chains."[127]

2) Provide human rights impact assessment of all contracts with Palantir

The government should commission an urgent independent review or parliamentary inquiry into the human rights compliance of Palantir and other high-profile companies involved in the response to Covid-19. This report should, among other aspects, assess the companies' human rights policies, compliance with international and national standards, and conduct a strict human rights impact assessment and investigation of their record. Given the importance of public trust in the government at this crucial time, government departments responsible for responding to Covid-19 should cease entering into new contracts with Palantir until the results of this independent review.

3) Increase transparency around contracts with Palantir and other tech companies.

The NHS/Palantir contracts were released only after immense pressure from civil society, and our FOIA Requests have revealed that a great deal of information about Palantir's access to our government is not easily accessible to the public. Increased public attention and education regarding the issue is crucial: foremost, all

[127] "Human Rights and Business 2017: Promoting responsibility and ensuring accountability – The UK's Government's approach to human rights and business", UK Human Rights (Joint Committee), UK Parliament, 4 April 2017, https://publications.parliament.uk/pa/jt201617/jtselect/jtrights/443/44307.htm.

government departments and public bodies with contracts with Palantir should make publicly available all such contracts, data sharing agreements, and related impact assessments. And these documents should be made public as standard for all public private partnerships of these kinds.

What you can do now

All these changes are vital. We can't wait for accountability. Sign this petition to make sure the Palantir/NHS datastore discussion gets the appropriate scrutiny in Parliament:

https://petition.parliament.uk/petitions/332714

ANNEX 1: PALANTIR RESPONSE TO THE REPORT

Dear Privacy International and No Tech For Tyrants:

By way of introduction, I work for Palantir Technologies and lead our in-house Gobal Privacy and Civil Liberties group. I have previously been in contact with some of your colleagues in response to an earlier open letter [privacyinternational.org] involving questions about our work with the UK's National Health Service (NHS). Today, I'm reaching out in response to your recent joint publication, All roads lead to Palantir: A review of how the data analytics company has embedded itself throughout the UK [privacyinternational.org].

As we've demonstrated repeatedly in the past, Palantir is committed to open and constructive dialogue with civil society groups and we welcome any opportunity to provide additional transparency into our business, technology, and, to the extent possible, our customer engagements. We therefore find it regrettable that Palantir was not offered the opportunity to address various assertions made in this report prior to its publication. Since no attempt was made to validate, clarify, or even request comment on contestable and thinly sourced claims, we are now calling attention to several assertions that are demonstrably false or misleading and/or perpetuate misrepresentations of our work that we have previously publicly clarified or corrected, including in our earlier response [privacyinternational.org]to your open letter.

Given both the severity and abundance of misrepresentations in your report, which we've documented below, we believe an immediate retraction is necessary. We request your prompt attention in rectifying

these misrepresentations and respectfully ask that you remove your currently posted report until an amended version addressing our points of contention and calls for corrections can be posted in its place. While other remediation paths may be available, it is our hope that for the sake of veracity, for the benefit of the public, and to support the legitimacy of your advocacy efforts you will be willing to work with us towards a timely resolution

For ease of reference, I have provided a series of direct quotes from your publication and noted below each the corresponding grounds for rectification:

1. **"...the United Kingdom's National Health Service (NHS) granted Palantir access to unprecedented quantities of health data for processing and analysis in response to Covid-19." [p.5]**

The framing of "granted Palantir access" is highly misleading: the NHS are using a secure and unique software instance - to which they control access - to process their own data. The only individuals who have access to this data are those specifically approved and granted access by the NHS; this does not extend to generalised Palantir access as the statement suggests.

As a data processor, Palantir Technologies UK provides software and support at the direction of our customers. If any Palantir UK engineers are granted limited access to a customer-controlled account to support a customer, their access must be specifically approved by that customer. Any data that the account contains remains under the control of the customer, and as such, the customer determines the manner in which data is processed and the purposes that this processing serves.

1. **"Palantir, by virtue of being a largely invisible "black box" technology provider, has operated under the radar in the UK until recently." [p.7]**

The claim that Palantir operates as a "largely invisible 'black box' technology provider" is undercut by the content of the very report in which it is posited. The document cites numerous sources, including public-facing technology and product descriptions, demonstrations, interviews, etc., all offering extensive details on Palantir software capabilities, uses, and customers.

1. **"Therefore, it appears from the above reports that both tools can process the exact same data in turn. Theoretically the learning system of one could thus be trained with the datasets incorporated in the other, especially when both tools are combined under a single platform." [p.12]**

The suggestion that the "learning system of one [platform] could thus be trained with the datasets incorporated in the other" is countermanded by the product descriptions it spuriously attempts to build upon. Nowhere in the preceding product descriptions is there evidence that Palantir relies on customer data to build "learning systems," transferable or otherwise. This is because the core of what Palantir's platforms provide are data integration and analysis capabilities that enable our customers to analyse their own data. Our platforms and our role as data processor are not based, focused, or reliant upon "learning systems" as implied by this statement.

1. **"When the New York Police Department (NYPD) tried to cancel its contract with Palantir and requested copies of the analyses of their data, Palantir refused to provide them in a standardised format that the NYPD would be able to use with their next system." [p.15]**

This statement is misleading. Palantir has always supported interoperability with standard, common use, and open data formats for data portability. Our approach to data openness and platform extensibility is rigorously documented here. The issue with NYPD was not around closed data formats, but the extent to which Palantir engineers would be directed, outside of contractual obligations, to support data

export functions and tasks that were readily available to NYPD technical staff.

1. **"On top of the revenue guaranteed by the extended contract, based on the part of the contract that has been made available, Palantir will be the intellectual property owner of any product developed for the NHS datastore project, including databases. This includes the ability to train other products using data processed through this contract, including people's sensitive personal data. Beyond the monetary compensation for the licensing of Palantir's product, Foundry, Palantir stands to gain massive amounts of potential training data for its tools." [p.16]**

This statement is categorically false. The NHS retains the intellectual property rights to its data, analyses, models, and other artifacts that may be produced using Palantir UK's software. This point has been directly clarified [nhsx.nhs.uk] by the NHS ("The contract contains the standard GCloud terms where relevant - any intellectual property rights derived from the work are reserved to the NHS.") We also addressed this point in a previous response [privacyinternational.org] to Privacy International ("Question: Will Palantir retain the NHS data analysis or insights gleaned from this contract once this exercise is over? Answer: No. As documented in the project's announcement [healthtech.blog.gov.uk], the NHS retains full ownership of NHS data and any analysis derived from this data.").

As noted in response to #3 above, this paragraph also fundamentally misunderstands our business model: we are a data management software provider, not an AI/ML vendor. We do not build or sell machine learning models as implied above. We have repeatedly sought to clarify this point in the public domain, including on our website.

The extent to which Palantir stands to "gain" from its exposure to customer environments is limited at best and categorically distinct from the mode implied by this false assertion. Like other SaaS providers, Palantir continuously works to improve its core software platforms, often

as a result of feedback from our users. If, for example, our work leads us to identify a software bug that needs to be resolved or ways in which a feature of our software can be made more user-friendly or accessible, we will make this improvement available to all of our customers. This is in no way equivalent to training proprietary models on specific customer data for retail to other customers, which we simply do not do.

1. **"Thus, it appears that through these "improvement" clauses, Palantir reserves itself the right to train its learning systems, including those of Gotham and Foundry and irrespective of whether these tools are sold as a combined solution or separately." [p.17]**

Similar to #5 above, this statement is false and fundamentally misrepresents the nature and architecture of our software. Foundry and Gotham are different and technically distinct offerings, and neither Foundry nor Gotham are learning systems as implied by this and previous statements, as has previously been clarified [privacyinternational.org]. Both Foundry and Gotham are data integration platforms that enable organisations to manage and analyse their own data. All data, and all insights derived from these data using our software, remain in our customers' ownership and under their control.

1. **"Palantir's services, including its signature Gotham platform, have been utilised by police forces across America and these agreements are reportedly sometimes established through backroom deals." [p.18]**

The supposed "backroom deals" allegation referred to here is false. The statement cites as evidence a 2018 article in *The Verge* regarding Palantir's *pro bono* support of the City of New Orleans' NOLA for Life murder reduction efforts. Claims of secrecy were debunked by a subsequent article in the Times Picayune [nola.com], which stated:

But the relationship is not exactly a secret. A Google search turns up the company's 2015 annual report in which it briefly summarizes its work in

New Orleans. Palantir is also mentioned on the city's NOLA For Life website, and in a 2016 NOLA For Life report [nolaforlife.org] that was presented to Williams, Guidry and their colleagues that same year. In both cases, the company is identified as a partner in the effort to "increase analytical capacity at NOPD."

Palantir, in its work with the City of New Orleans, has been open and transparent since the start of the engagement. Both Palantir and the City of New Orleans adhered to standard procurement rules and procedures in all phases of the partnership.

1. **"Palantir has faced significant public criticism for its contracts with US Immigration and Customs Enforcement (ICE), an agency under the US Department of Homeland Security (DHS), who have faced significant outcry over their policy of separating children from their families, and keeping them in horrific conditions." [p.28]**

The statement as framed is factually inaccurate and misleading. As we have stated publicly [amnesty.org.nz], Palantir has contracts only with the criminal investigative division of ICE and DHS at large – called Homeland Security Investigations (HSI), which began in 2011 under President Barack Obama. HSI uses Palantir software platforms to assist in analysing its data to achieve its mission – primarily focused on combatting transnational crime such as money laundering, transnational gang activity, child exploitation, human smuggling, terrorist threats, and more. Palantir has no contract with the Enforcement and Removal Operations (ERO) division of ICE. It is ERO, not HSI, that 'identifies and apprehends removable aliens, detains these individuals when necessary and removes illegal aliens from the United States' as its primary mission. Furthermore, Palantir has had no involvement whatsoever in the management or operation of any of ERO's detention centers. Palantir also has no contracts with U.S. Customs and Border Protection (CBP). CBP was responsible for the Trump Administration's 'zero tolerance' family separation policies initiated and ended in 2018. Palantir continues to regard that policy, which resulted in the separation of children from

parents and the incarceration or 'caging' of children, as abhorrent – violating basic human decency and human rights standards. Palantir also has had no involvement in the management or operation of any of CBP's detention centers at the border.

1. **"The Palantir–supplied predictive policing software suite, known as Hessendata, triangulates a number of distinct datasets from police and other databases, including social media, enabling the automated analysis of potential suspects." [p.30]**

This statement includes factual misrepresentations and misleading insinuations. The Palantir platform licensed to the Hessen State police is not a "predictive policing software suite." On the contrary, Palantir's software is used to analyse data and evidence available and acquired in the course of regular police investigations, in this case focused on serious and organised crime. Moreover, inclusion of social media data is not, as the phrasing suggests, generalised and indiscriminate, but rather would only take place in the context of specific investigations and typically produced as a result of criminal warrant or other legal process request. Finally, the suggestion that Palantir software is "enabling the automated analysis of potential suspects" fundamentally misconstrues the functionality and use of the platform provided to our law enforcement customers, including the Hessen police. Far from automating analysis, the platform is used by law enforcement analysts and investigators to support their direct, manually guided, human-driven analytics and case development efforts.

1. **"Circumventing the GDPR through a national exemption, the contract, which was signed for 84 months, gives the PET and the Police the ability to allegedly predict likely cases of terrorism before they occur. It is currently unclear exactly what variables are used, how data is parsed, and when something might flag up as a potential threat." [pp.31-32]**

This statement is misleading on several points and fundamentally misrepresents the core architecture of EU data protection law. To the

extent the Danish National Police processes personal data for law enforcement purposes, the EU Law Enforcement Data Protection Directive applies, rather than the GDPR. As every other EU country, Denmark had to transpose the Directive into Danish national law to take effect. In so doing, Denmark established a robust data protection regime that applies to and is adhered to by the Danish National Police. Among others, Chapter 12 of law no. 410 of 27 April 2017 on the processing of personal data by law enforcement authorities [retsinformation.dk] establishes explicit rules around the security and appropriateness of personal data processing in automated systems, including the prevention of unauthorized access to sensitive data. The law also imposes extensive oversight requirements, including the ability to audit who had access to, or entered data into the system. Palantir is proud to build and provide platforms able to meet these and other data protection requirements.

The claim that POL-INTEL is used to "predict likely cases of terrorism before they occur" is factually incorrect. Palantir is used across many categories of major crimes, but does not include any individualised "predictive" capabilities and instead allows the Danish National Police to utilise data that they have existing, legal access to in pursuit of major criminal investigations, as well as enabling their Data Protection Unit to ensure accountable system use through the analysis of system audit logs.

1. "This is further compounded by their Palantir contract, which enables the WFP to generate wide-scale insights, with the risk of seriously compromising the privacy of aid recipients, and in turn present Palantir with the opportunity to deploy, test, and improve their products on the back on fragile populations in contexts of suspended or limited rights. PI have questioned this partnership in the past, not least because of its potential violation of a principle of humanitarian action, namely that agencies are neutral." [p.32]

Like previous statements, this fundamentally misunderstands the nature of

Palantir's software development practices and the work our software enables for customers across the government, commercial, and humanitarian sectors. Palantir deploys our commercially available data integration platform, Foundry, in an environment where access and use are controlled by the WFP. Palantir is proud to be able to support the life-saving work of the WFP and to help provide a model for others in the humanitarian space in how to leverage data to serve fragile populations quickly, humanely, responsibly, and effectively as they confront famine around the world.

1. **"They claim they are working hard to create a better society that preserves privacy and civil liberties and avoid mistaking algorithms for universal solutions to ethical problems. Palantir appears is [sic] conducting due diligence on paper. The next section highlights what needs to be done for this veneer of respect for privacy, liberty and civil rights to be verified and upheld in practice. "**

Had Privacy International and No Tech For Tyrants sought to engage with Palantir UK directly regarding the concerns raised in their report, we might have had an opportunity to explain and demonstrate the multitude of investments — due diligence efforts, cultural trainings, privacy engineering practices, scholarship, community engagement, etc. — that contribute to our rigorous approach to addressing the legal, ethical, and normative dimensions of our work.

As we have stated elsewhere [amnestyusa.org], we acknowledge that our work in supporting the missions and enabling solutions to the data challenges faced by our customers carries with it real responsibilities. That is a price of working in the real world with critical and often imperfect institutions. We neither shy away from these responsibilities nor attempt to hide behind assertions of being a mere technology vendor. On the contrary, we soberly accept that responsibility, are prepared to address legitimate concerns grounded in substantiated facts, and remain open to

honest and constructive dialogue on these issues with any members of civil society willing to engage with us in good faith. Should your organisations develop an appetite to engage in good faith on these difficult issues, we stand ready as willing partners.

For now, we respectfully request your timely efforts to amend your report to reflect the clarifications and corrections outlined above.

ANNEX 2: PI AND NT4T RESPONSE TO PALANTIR

Our answers:

The (NT4T and PI) report says:

1. "...the United Kingdom's National Health Service (NHS) granted Palantir access to unprecedented quantities of health data for processing and analysis in response to Covid-19." [p.5]

You (Palantir) said:

> *The framing of "granted Palantir access" is highly misleading: the NHS are using a secure and unique software instance - to which they control access - to process their own data. The only individuals who have access to this data are those specifically approved and granted access by the NHS; this does not extend to generalised Palantir access as the statement suggests.*
>
> *As a data processor, Palantir Technologies UK provides software and support at the direction of our customers. If any Palantir UK engineers are granted limited access to a customer-controlled account to support a customer, their access must be specifically approved by that customer. Any data that the account contains remains under the control of the customer, and as such, the customer determines the manner in which data is processed and the purposes that this processing serves.*

Our (NT4T and PI) Response:

The explanation provided by Palantir does not contradict our statement. All we are saying is that Palantir, as the company concedes in its response, does have access

to the data, whether it is via the software or its employees. We are not denying that Palantir is acting as a data processor.

The report says:

2. “Palantir, by virtue of being a largely invisible “black box” technology provider, has operated under the radar in the UK until recently." [p.7]

You said:

> *The claim that Palantir operates as a “largely invisible ‘black box’ technology provider” is undercut by the content of the very report in which it is posited. The document cites numerous sources, including public-facing technology and product descriptions, demonstrations, interviews, etc., all offering extensive details on Palantir software capabilities, uses, and customers.*

Our Response:

The information pulled together for the purposes of this report was the result of painstaking efforts by many groups to obtain records of Palantir’s contracts with UK government authorities. To our knowledge, neither the government nor Palantir made all this information available on their own initiative. If Palantir’s intent is to become more transparent as to its capabilities, uses, and customers, we welcome that development, but stand by the accuracy of the statement in the report.

The report said:

3. “Therefore, it appears from the above reports that both tools can process the exact same data in turn. Theoretically the learning system of one could thus be trained with the datasets incorporated in the other, especially when both tools are combined under a single platform.” [p.12]

You said:

> *The suggestion that the "learning system of one [platform] could thus be trained with the datasets incorporated in the other" is countermanded by the product descriptions it spuriously attempts to build upon. Nowhere in the preceding product descriptions is there evidence that Palantir relies on customer data to build "learning systems," transferable or otherwise. This is because the core of what Palantir's platforms provide are data integration and analysis capabilities that enable our customers to analyse their own data. Our platforms and our role as data processor are not based, focused, or reliant upon "learning systems" as implied by this statement.*

Our Response:

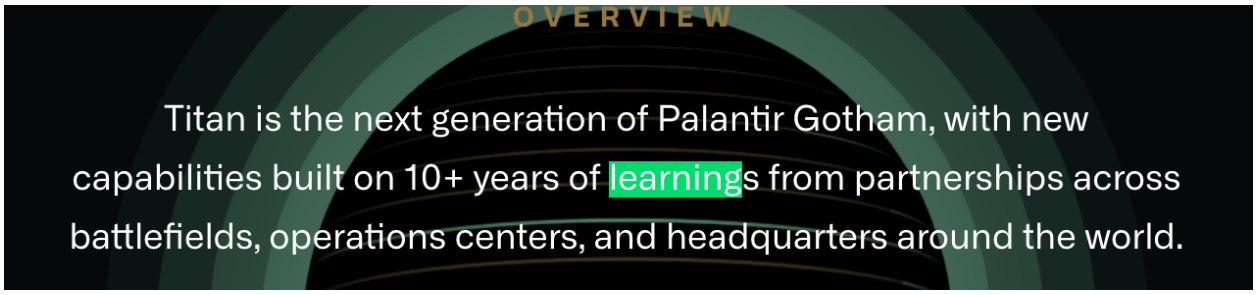
We do not state that Palantir was solely reliant upon "learning systems", but that the processing of one system could be used to build models for either system.

The diverse datasets parsed through Foundry could enable Palantir to experiment with, learn from, and improve the product's ability to integrate with multifarious AI models, and to apply data transformation and normalisations in different ways. Foundry's product page states that users can: "[…] accelerate machine learning and artificial intelligence with quality data and seamless deployment to production".

Moreover, although Foundry and Gotham are not themselves learning systems, Palantir does, according to these contracts, have the right to improve both systems using learnings from the data they have gathered. It stands to reason that significant R&D value is generated from the use of Foundry in the context of the NHS contract.

The fact that Palantir uses insight from its current deployments of Gotham to improve and develop software is not a secret - it's a specific part of Palantir's

marketing.



The report says:

4. "When the New York Police Department (NYPD) tried to cancel its contract with Palantir and requested copies of the analyses of their data, Palantir refused to provide them in a standardised format that the NYPD would be able to use with their next system." [p.15]

You said:

> *This statement is misleading. Palantir has always supported interoperability with standard, common use, and open data formats for data portability. Our approach to data openness and platform extensibility is rigorously documented here. The issue with NYPD was not around closed data formats, but the extent to which Palantir engineers would be directed, outside of contractual obligations, to support data export functions and tasks that were readily available to NYPD technical staff.*

Our response:

In June of 2017 Buzzfeed reported on an argument between Palantir and the NYPD.

"The NYPD asked Palantir in February for a copy of this analysis, and for a translation key so that it could put the analysis into its Cobalt system, the people familiar with the matter said. But when Palantir delivered a file in May, it declined to provide a way to translate it, arguing that doing so would require exposing its intellectual property, the people said.

The NYPD then asked Palantir for the information in a translated format — asking Palantir to do the translation itself — according to the people. Palantir responded this month, providing a file that was indeed readable. But according to the NYPD's examination of the file, it contained only the original data the NYPD had fed into the system, the people said. The analysis appeared to be missing."

We don't believe that we've misrepresented this argument. If there is further information you can provide, which would clarify these concerns, we would be interested to hear it.

Report modification:

- We have added 'reportedly'

Updated report: "When the New York Police Department (NYPD) tried to cancel its contract with Palantir and requested copies of the analyses of their data, Palantir reportedly refused to provide them in a standardised format that the NYPD would be able to use with their next system."

The report says:

5. "On top of the revenue guaranteed by the extended contract, based on the part of the contract that has been made available, Palantir will be the intellectual property owner of any product developed for the NHS datastore project, including databases. This includes the ability to train other products using data processed through this contract, including people's sensitive personal data. Beyond the monetary compensation for the licensing of Palantir's product, Foundry, Palantir stands to gain massive amounts of potential training data for its tools." [p.16]

You said:

> *This statement is categorically false. The NHS retains the intellectual property rights to its data, analyses, models, and other artifacts that may be produced using Palantir UK's software. This point has been directly clarified by the NHS ("The contract contains the standard GCloud terms where*

relevant - any intellectual property rights derived from the work are reserved to the NHS.") We also addressed this point in aprevious response to Privacy International ("Question: Will Palantir retain the NHS data analysis or insights gleaned from this contract once this exercise is over? Answer: No. As documented in the project's announcement, the NHS retains full ownership of NHS data and any analysis derived from this data.").

As noted in response to #3 above, this paragraph also fundamentally misunderstands our business model: we are a data management software provider, not an AI/ML vendor. We do not build or sell machine learning models as implied above. We have repeatedly sought to clarify this point in the public domain, including on our website.

The extent to which Palantir stands to "gain" from its exposure to customer environments is limited at best and categorically distinct from the mode implied by this false assertion. Like other SaaS providers, Palantir continuously works to improve its core software platforms, often as a result of feedback from our users. If, for example, our work leads us to identify a software bug that needs to be resolved or ways in which a feature of our software can be made more user-friendly or accessible, we will make this improvement available to all of our customers. This is in no way equivalent to training proprietary models on specific customer data for retail to other customers, which we simply do not do.

Our response:

Please see point #3 for our response re learning systems.

While Palantir has stated "all data, and all insights derived from these data using our software, remain in our customers' ownership and under their control", clause 11.2 of the Palantir contract grants NHS non-exclusive, royalty-free licence to use Project Specific IPRs.

"11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background

IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities"

Therefore, as it currently stands, Palantir are in a position to benefit from Project Specific IPRs, in spite of afore-mentioned assurances. Can you clarify if this is not the case?

Report modification:

- We removed the first sentence to avoid any misunderstanding with regard to the Palantir-NHS arrangement.
- We further added the exact wording of the NHS contract to avoid any misunderstanding and revised language on that:

"Only following a legal challenge initiated by civil society, were the contracts released, clause 11.2 of the disclosed contract stipulates that "The Supplier [Palantir] grants the Buyer [NHS] a non-exclusive, transferable, perpetual, irevocalbe, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Projet Specific IPRs for the Buyer's ordinary business activities."

- We have now changed 'train' to 'improve' as we acknowledge that 'train' could be confusing and further modified the text of the paragraph.

Updated report: "On top of the revenue guaranteed by the extended contract, based on the part of the contract that has been made available, NHS will not be the intellectual property owner of the product developed for the NHS datastore projects. Only following a legal challenge initiated by civil society, were the contracts reportedly released, clause 11.2 of the disclosed contract stipulates that "The Supplier [Palantir] grants the Buyer [NHS] a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities." This means that Palantir retains intellectual property rights in the products it specifically develops for the NHS, while also licensing those rights to them. Beyond the monetary compensation for the licensing of Palantir's product, Foundry, Palantir

stands to gain further insight and the ability to improve Foundry based on the NHS deployment."

The report says:

6. "Thus, it appears that through these "improvement" clauses, Palantir reserves itself the right to train its learning systems, including those of Gotham and Foundry and irrespective of whether these tools are sold as a combined solution or separately." [p.17]

You said:

> *Similar to #5 above, this statement is false and fundamentally misrepresents the nature and architecture of our software. Foundry and Gotham are different and technically distinct offerings, and neither Foundry nor Gotham are learning systems as implied by this and previous statements, as has previously been clarified. Both Foundry and Gotham are data integration platforms that enable organisations to manage and analyse their own data. All data, and all insights derived from these data using our software, remain in our customers' ownership and under their control.*

Our response:

See point #3 re learning systems. We have now changed 'train its learning systems' to 'improve its systems' as we acknowledge that the original wording may be confusing.

We believe the confusion here is the word 'combined'. We absolutely understand that Foundry and Gotham are different software (although it is difficult to tell in what ways their operations are distinct based on online information - so any information you could provide would be extremely useful). The point we are trying to make here is that the systems are interoperable, and that learnings from one could potentially inform the use and improvements in the other.

What we have understood from the Center for Advanced Defense Studies is that the two systems work very well together. And, from Robert Fink, one of the designers of Foundry, that all the Palantir products share the same database backend called AtlasDB.

As you can see from our answer to point #3 - that Palantir uses information from people's usage to improve their systems does not seem to be a secret, and is confirmed in the project announcement for Gotham's new update Titan.

Report modification:

- We have now changed 'train its learning systems' to 'improve its system' recognising that the chosen language may be misinterpreted.

Updated report: "Thus, it appears that through these "improvement" clauses, Palantir reserves itself the right to improve its systems, including those of Gotham and Foundry and irrespective of whether these tools are sold as a combined solution or separately."

The report says:

7. "Palantir's services, including its signature Gotham platform, have been utilised by police forces across America and these agreements are reportedly sometimes established through backroom deals." [p.18]

You said:

> *The supposed "backroom deals" allegation referred to here is false. The statement cites as evidence a 2018 article in The Verge regarding Palantir's pro bono support of the City of New Orleans' NOLA for Life murder reduction efforts. Claims of secrecy were debunked by a subsequent article in the Times Picayune, which stated:*
> *But the relationship is not exactly a secret. A Google search turns up the company's 2015 annual report in which it briefly summarizes its work in New Orleans. Palantir is also mentioned on the city's NOLA For Life website, and in*

> *a 2016 NOLA For Life report that was presented to Williams, Guidry and their colleagues that same year. In both cases, the company is identified as a partner in the effort to "increase analytical capacity at NOPD."*
> *Palantir, in its work with the City of New Orleans, has been open and transparent since the start of the engagement. Both Palantir and the City of New Orleans adhered to standard procurement rules and procedures in all phases of the partnership.*

Our Response:

We don't believe that a backroom deal must, necessarily, involve absolute secrecy - though we concede the term is subjective. Instead, we would argue that a backroom deal lacks transparency and due process, which we (PI and NT4T) believe are imperative throughout all public-private partnerships. Effective transparency and due process in public-private partnerships includes providing information before the deal is signed. Additionally, transparency requires that information on the specifics of such partnerships should be accessible to the public. Information on the data a company's product has access to, what role the company's product or service performs in the decision-making process, whether risk assessments were conducted, how the company benefits from this agreement, whether there are other agreements. Public-private partnerships should be open to public scrutiny.

We would appreciate if you could provide us further clarifications on the matter. The Verge reported that "Thanks to its philanthropic status, as well as New Orleans' "strong mayor" model of government, the agreement never passed through a public procurement process." We would appreciate any further details or clarification you could provide. Was this a result of Palantir offering its services pro bono?

The article you shared with us in the response further raises concerns regarding the need for oversight, transparency and community support. Could you please provide further information on how these concerns were addressed?

If you agree that transparency is important to ensure public confidence and accountability, we also ask that you disclose a customer list detailing your government partnerships.

The report says:

8. "Palantir has faced significant public criticism for its contracts with US Immigration and Customs Enforcement (ICE), an agency under the US Department of Homeland Security (DHS), who have faced significant outcry over their policy of separating children from their families, and keeping them in horrific conditions." [p.28]

You said:

> *The statement as framed is factually inaccurate and misleading. As we have stated publicly, Palantir has contracts only with the criminal investigative division of ICE and DHS at large – called Homeland Security Investigations (HSI), which began in 2011 under President Barack Obama. HSI uses Palantir software platforms to assist in analysing its data to achieve its mission – primarily focused on combatting transnational crime such as money laundering, transnational gang activity, child exploitation, human smuggling, terrorist threats, and more. Palantir has no contract with the Enforcement and Removal Operations (ERO) division of ICE. It is ERO, not HSI, that 'identifies and apprehends removable aliens, detains these individuals when necessary and removes illegal aliens from the United States' as its primary mission. Furthermore, Palantir has had no involvement whatsoever in the management or operation of any of ERO's detention centers. Palantir also has no contracts with U.S. Customs and Border Protection (CBP). CBP was responsible for the Trump Administration's 'zero tolerance' family separation policies initiated and ended in 2018. Palantir continues to regard that policy, which resulted in the separation of children from parents and the incarceration or 'caging' of children, as abhorrent – violating basic human decency and human rights standards. Palantir also has had no involvement in the management or operation of any of CBP's detention centers at the border.*

Our response:

US Immigration and Customs Enforcement (ICE), an agency under the US Department of Homeland Security (DHS) have faced significant outcry over their

policy of separating children from their families, and keeping them in horrific conditions. Nowhere in the statement above do we explicitly state that Palantir's product was used for child separation. We have added an acknowledgement of your response in the report.

The report says:

9. "The Palantir–supplied predictive policing software suite, known as Hessendata, triangulates a number of distinct datasets from police and other databases, including social media, enabling the automated analysis of potential suspects." [p.30]

You said:

> *This statement includes factual misrepresentations and misleading insinuations. The Palantir platform licensed to the Hessen State police is not a "predictive policing software suite." On the contrary, Palantir's software is used to analyse data and evidence available and acquired in the course of regular police investigations, in this case focused on serious and organised crime. Moreover, inclusion of social media data is not, as the phrasing suggests, generalised and indiscriminate, but rather would only take place in the context of specific investigations and typically produced as a result of criminal warrant or other legal process request. Finally, the suggestion that Palantir software is "enabling the automated analysis of potential suspects" fundamentally misconstrues the functionality and use of the platform provided to our law enforcement customers, including the Hessen police. Far from automating analysis, the platform is used by law enforcement analysts and investigators to support their direct, manually guided, human-driven analytics and case development efforts.*

Our response:

Please see our response on #10.

Report modification:

- We have now removed 'predictive' and 'automated' to avoid any misunderstanding and added 'reportedly'.

Updated report: "The Palantir–supplied policing software suite, known as Hessendata, reportedly triangulates a number of distinct datasets from police and other databases, including social media, enabling the analysis of potential suspects."

The report says:

10. "Circumventing the GDPR through a national exemption, the contract, which was signed for 84 months, gives the PET and the Police the ability to allegedly predict likely cases of terrorism before they occur. It is currently unclear exactly what variables are used, how data is parsed, and when something might flag up as a potential threat." [pp.31-32]

You said:

> *This statement is misleading on several points and fundamentally misrepresents the core architecture of EU data protection law. To the extent the Danish National Police processes personal data for law enforcement purposes, the EU Law Enforcement Data Protection Directive applies, rather than the GDPR. As every other EU country, Denmark had to transpose the Directive into Danish national law to take effect. In so doing, Denmark established a robust data protection regime that applies to and is adhered to by the Danish National Police. Among others, Chapter 12 of law no. 410 of 27 April 2017 on the processing of personal data by law enforcement authorities establishes explicit rules around the security and appropriateness of personal data processing in automated systems, including the prevention of unauthorized access to sensitive data. The law also imposes extensive oversight requirements, including the ability to audit who had access to, or entered data into the system. Palantir is proud to build and provide platforms*

able to meet these and other data protection requirements.
The claim that POL-INTEL is used to "predict likely cases of terrorism before they occur" is factually incorrect. Palantir is used across many categories of major crimes, but does not include any individualised "predictive" capabilities and instead allows the Danish National Police to utilise data that they have existing, legal access to in pursuit of major criminal investigations, as well as enabling their Data Protection Unit to ensure accountable system use through the analysis of system audit logs.

Our response:

While the Danish police deny that they are performing predictive policing, they are engaged in what they call "hotspot mapping", which underscores that this is a definitional question, as opposed to a functional one. In the public tender, shared by Algorithm Watch that the Danish government issued, product requirements included:

Registers of information such as incidents and criminal matters as well as document management systems

- Case management systems
- Investigation support systems
- Forensics and mobile forensics systems
- Open source retrieval systems
- The analytical platform is requested to support the exchange of information with national and international partners (e.g. Interpol and Europol) and be able to load and import data from ad-hoc extraction, typically used in exploration

On the definitional question, Palantir Gotham, as described by Palantir, has a "heatmap" function, that categorises "objects" (across a number of datasets) on a map.

As explained below, this is considered as one of different categories of "predictive policing" – which does not have one agreed-upon universal definition.

The RAND Corporation broadly structures predictive policing techniques in four classes:

1. Classical statistical techniques: This class includes standard statistical processes, such as most forms of regression, data mining, time-series analysis, and seasonality adjustments.

2. Simple methods: Simple methods do not require much in the way of sophisticated computing or large amounts of data. Most heuristic methods, for example, are simple methods—relying more on checklists and indexes than on the analysis of large data sets.

3. Complex applications: These applications include new and innovative methods or methods that require considerable amounts of data in addition to sophisticated computing tools. Many newer data mining methods and some near-repeat methods fall into this class.

4. Tailored methods: In several cases examined here, existing techniques were adapted to support predictive policing. For example, classical statistical methods can be used to produce heat maps, which are simple, color-coded grids depicting the intensity of crime activity in a given area.

The last policing technique mentioned above, the tailored method, seems to include the method that is according to the company used by Palantir Gotham and has been reported as such.

The RAND Corporation defines hot spot methods as: "Hot spot methods predict areas of increased crime risk based on historical crime data. Hot spot methods seek to take advantage of the fact that crime is not uniformly distributed, identifying areas with the highest crime volumes or rates. The underlying assumption—and prediction—is that crime will likely occur where crime has already occurred: The past is prologue"

See also sources:
https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd

Report modification:

- We corrected the reference to 'GDPR' with the 'EU Law Enforcement Directive' as indeed this will be the correct legal framework applicable in this case.
- We replaced 'predictive' with 'identify' to avoid any misunderstanding.

Updated report: "Circumventing the EU Law Enforcement Directive through a national exemption, the contract, which was signed for 84 months, gives the PET and the Police the ability to allegedly identify likely cases of terrorism before they occur.[128] It is currently unclear exactly what variables are used, how data is parsed, and when something might flag up as a potential threat."

The report says:
11. "This is further compounded by their Palantir contract, which enables the WFP to generate wide-scale insights, with the risk of seriously compromising the privacy of aid recipients, and in turn present Palantir with the opportunity to deploy, test, and improve their products on the back on fragile populations in contexts of suspended or limited rights. PI have questioned this partnership in the past, not least because of its potential violation of a principle of humanitarian action, namely that agencies are neutral." [p.32]

You said:

> *Like previous statements, this fundamentally misunderstands the nature of Palantir's software development practices and the work our software enables for customers across the government, commercial, and humanitarian sectors.*

[128] This type of identification techniques is described by some as predictive policing. See our full answer to Palantir on point 10, Annex 2 to this report.

Palantir deploys our commercially available data integration platform, Foundry, in an environment where access and use are controlled by the WFP. Palantir is proud to be able to support the life-saving work of the WFP and to help provide a model for others in the humanitarian space in how to leverage data to serve fragile populations quickly, humanely, responsibly, and effectively as they confront famine around the world.

Our response: Please see our answers above #3, #5 and #6.

The report says:

12. "They claim they are working hard to create a better society that preserves privacy and civil liberties and avoid mistaking algorithms for universal solutions to ethical problems. Palantir appears is [sic] conducting due diligence on paper. The next section highlights what needs to be done for this veneer of respect for privacy, liberty and civil rights to be verified and upheld in practice."

You said:

Had Privacy International and No Tech For Tyrants sought to engage with Palantir UK directly regarding the concerns raised in their report, we might have had an opportunity to explain and demonstrate the multitude of investments — due diligence efforts, cultural trainings, privacy engineering practices, scholarship, community engagement, etc. — that contribute to our rigorous approach to addressing the legal, ethical, and normative dimensions of our work.

As we have stated elsewhere, we acknowledge that our work in supporting the missions and enabling solutions to the data challenges faced by our customers carries with it real responsibilities. That is a price of working in the real world with critical and often imperfect institutions. We neither shy away from these responsibilities nor attempt to hide behind assertions of being a mere technology vendor. On the contrary, we soberly accept that responsibility, are prepared to address legitimate concerns grounded in

substantiated facts, and remain open to honest and constructive dialogue on these issues with any members of civil society willing to engage with us in good faith. Should your organisations develop an appetite to engage in good faith on these difficult issues, we stand ready as willing partners.

Our response:

We would be happy to be provided with more information and documents on what exact due diligence and risk/impact assessments the company undertakes before and while engaging with operations that might bear human rights risks for certain populations. We look forward to receiving your responses to our questions.

In order to assist us in moving forward, we would be grateful if you could provide further clarification on the points you raised in your email and on others raised in the report. For ease of reference, we have collated our questions and requests for further information here:

- We ask to please provide further information in regard to your contract with the NYPD, which would clarify concerns around data.
- As it currently stands, it seems that Palantir are in a position to benefit from the NHS-Palantir partnership, in spite of afore-mentioned assurances. Can you clarify if this is not the case?
- In order to provide transparency to the public and help PI, NT4T and others have a better understanding of Palantir's work and concerns, we ask that you disclose a customer list detailing your government partnerships.
- We would also be interested to receive more information and documents on what exact due diligence and risk/impact assessments the company undertakes before and while engaging with operations that might bear human rights risks for certain populations.