The Shadow Contract, Episode Three: Drag and Drop

If you're listening to this, it means you care about the truth. At Good Law Project, we don't just expose wrongdoing, we go to court to stop it. From secret NHS data deals, to PPE cronyism, to environmental destruction quietly signed off by the government, we uncover what's hidden, hold power to account and use the law to resist hate and bring hope. But here's the truth. We can only keep protecting you and exposing stories like this one if you stand with us. We don't take corporate money, we answer to no party or private interest. We're people powered. We're funded by people like you. Injustice is not inevitable. So if you believe in truth, accountability and the right to know what's being done in your name, support our work. Go to **goodlawproject.org/podcast** and give what you can. Because if we don't fight for transparency, who will?

Rhiannon Mihranian Osborne: "The Home Office has wanted migrants' data, health data, for years and has a little bit of it and is dying to get more. The UK government is in the context of massively wanting to expand their ability to police and deport people. And Palantir is a perfect partner for all of this, who now has access to huge amounts of health data as well. So it wouldn't take loads, you know, some changes in legislation, some ignoring of legislation for a current or future government to say, okay, well, we're going to combine these data sources now and, you know, find the protesters we don't like and find the undocumented migrants we want to deport."

In the last episode, we saw how Palantir quickly and quietly insinuated itself into the NHS under the cover of a global pandemic, leveraging a £1 emergency contract into a £330 million play to build a hallowed new Federated Data Platform. And while CIOs and hospital managers fawned over shiny new software dashboards, Palantir positioned itself at the

centre of one of the NHS's most valuable assets: the system that organises, controls and analyses our health data.

I'm Eliza Pitkin and this is The Shadow Contract, episode three: Drag and Drop.

We know that our patient data, if used well, could transform care across the NHS and even the world, improving outcomes and saving lives. But that data, once connected, standardised and made searchable at scale, that data, insufficiently anonymised and safeguarded, could be dangerous.

Because the same systems that help plan services and spot risk can just as easily be adapted to identify, prioritise and target people. And once that capability exists, the question is no longer whether it can be used, but how it's used. Champions of Palantir's version of the FDP insist that it's being built in the name of efficiency and care, speaking out harshly against critics' concerns and accusing them of putting ideology before patient care. But we know that elsewhere, Palantir's technology has already been used to connect health and benefits data with enforcement systems, powering tools that support immigration crackdowns across the United States.

So as Palantir moves closer to the centre of the NHS's data architecture, we ask what safeguards really exist to stop the same patterns, the same pressures and the same outcomes from taking hold here. We take a closer look at why we should all be really, really worried about Palantir, because to be very clear, the call is coming from inside the house.

In the United States, Palantir's DNA is deeply woven into the government data systems. Since the company's founding, its Gotham and Foundry platforms, originally developed for counterterrorism and intelligence analysis, became staples across US national security agencies, linking once separate databases for the CIA, NSA, FBI and Department of Defense to enable cross-agency analysis and battlefield decision-making.

Over the last decade, that relationship expanded into immigration enforcement and domestic security. Palantir first built an investigative

case management system for Immigration and Customs Enforcement, also known as ICE, in 2014. A contract that's since evolved and grown, Palantir has cemented its position across US defence infrastructure. In 2025, the US Army awarded a $10 billion enterprise contract spanning a decade to consolidate and expand AI, analytics and data fusion systems across multiple military programmes, the largest government agreement in the company's history.

Against that backdrop, where one vendor's software underpins everything from battlefield logistics to immigration case management, concerns about how data is used, combined and repurposed have become central to debates about civil liberties, transparency and the balance between public good and state power.

Recent activity in the US blurs the vital line between care and enforcement to a terrifying degree and forces us to question even more urgently how our own patient data might be used, not just by Palantir, but by our own government.

Because in mid 2025, Palantir rolled out an analytics application known as ELITE. ELITE pulls together information from federal sources and government health data, like Medicaid, to create leads to be used by ICE in enforcement activity. By the way, ELITE stands for Enhanced Leads Identification and Targeting for Enforcement. It's gross.

So instead of information remaining securely within the health or benefit system it was collected for, ELITE maps address and identity data from Medicaid and other records and aligns it with immigration data. The result is a system that produces searchable maps, individual profiles and so-called confidence scores, estimates of whether a person is likely to be at a particular address, which are then used to plan and prioritise field operations. If you remember our Tony Blair example from episode two, it's fair to say that ICE would be around Tony's house in a hot minute if his papers weren't up to date.

Privacy advocates, including the Electronic Frontier Foundation, have warned about what this represents. Data collected to provide healthcare

and public support is being repurposed for enforcement, raising serious questions about consent, trust and the boundaries between care and control. One of the most immediate concerns is that people who rely on Medicaid may avoid seeking healthcare altogether if they believe their information could be used to locate them for detention or deportation.

The EFF has gone further, taking legal action to challenge the flow of Medicaid data to ICE. Their warning is blunt, that systems like ELITE are exactly the kind of surveillance superstructures civil liberties protections were meant to prevent. And this prophetic example isn't unusual. It's very much Palantir's MO and it doesn't stop at ELITE.

Under a $30 million contract, Palantir is building Immigration OS, a system designed to give ICE near real-time visibility into immigrant cases by consolidating biometric and federal data into a single operational platform. It's the same structural pattern. Disparate public data sources pooled, searchable, actionable, not passive record keeping, active prioritisation. Aggregating data sources, some of them collected for unrelated public service purposes, into a searchable, actionable repository used to drive state action.

Advocacy groups and civil liberties organisations argue that systems like Immigration OS extend the role of integrated data platforms from passive record keeping into the realm of active prioritisation and targeting – raising similar concerns about mission creep, privacy and transparency, that have been voiced in debates over health data systems like the NHS' Federated Data Platform.

Not close enough to home? In the UK, we've already seen how this kind of infrastructure can take shape inside policing. Reporting by Liberty Investigates and the i revealed that Palantir worked with several English peace forces on a project known as Nectar, a real-time data sharing and analysis network for law enforcement.

Internal documents showed it was designed to pull together dozens of data sources, combining police intelligence with highly sensitive personal information from elsewhere in the public sector, including health data and

markers of political or philosophical belief. Once ingested, that information became searchable, linkable and operational in real time. Not a static database; an active analytical environment.

Let's be very clear here. We aren't talking about opportunistic exploitation of a system by bad actors. We are talking about a very deliberate and planned strategy by Palantir. We are talking about software systems that have this interoperability built into them. Because at the heart of the FDP and countless other Palantir systems around the world, beats Foundry, a data integration and analytics platform: a system built to pull together vast amounts of data from different sources, structure it, model it and turn it into what Palantir calls a quote: "common operating picture".

In a healthcare setting, that sounds pretty useful, essential even. The ability to see and manage waiting lists, bed capacity, discharge delays, all in one place. By design, Foundry allows for the literal drag and drop of this data. Not just across the modules within a system like the FDP, but into any Foundry platform with the potential for that data to be shared and used far beyond where it was originally intended or permitted.

This drag and drop capability even extends as far as Gotham, Palantir's defense, intelligence and law enforcement operations platform. And this isn't via some nefarious backdoor exploitation or hack. This is by design.

In the words of Louis Mosley, head of Palantir UK and Europe in his testimony to the House of Commons Science, Innovation and Technology Committee in July 2025, quote: "Foundry is used in military contexts alongside Gotham. That is why those two platforms are interoperable so that moving data and other applications between the two is seamless."

So when we talk about drag and drop, we're not talking about a user friendly feature. We're talking about infrastructure that allows data environments to connect across contexts. Healthcare on one side, military and intelligence tooling on the other. Governance frameworks may promise limits. Contracts may define scope. But technically, structurally, the systems are built to be able to talk to each other.

And this is where a term that once felt fringe is entering serious democratic debate: Technofascism. No jackboots, no tanks on streets. Technofascism describes the fusion of advanced data infrastructure with concentrated state power where mass data collection, AI modeling and predictive systems are used to categorise, monitor and control populations at scale. It isn't about dramatic authoritarian takeovers. It's about the quiet normalisation of total visibility.

If you're listening to this, it means you care about the truth. At Good Law Project, we don't just expose wrongdoing, we go to court to stop it. From secret NHS data deals, to PPE cronyism, to environmental destruction quietly signed off by the government, we uncover what's hidden, hold power to account and use the law to resist hate and bring hope. But here's the truth. We can only keep protecting you and exposing stories like this one if you stand with us. We don't take corporate money, we answer to no party or private interest. We're people powered. We're funded by people like you. Injustice is not inevitable. So if you believe in truth, accountability and the right to know what's being done in your name, support our work. Go to **goodlawproject.org/podcast** and give what you can. Because if we don't fight for transparency, who will?

Rhiannon Mihranian Osborne is a Bertha Challenge Fellow, investigating the intersection of big tech, government power and democratic oversight. She's very clear about Palantir's game plan with systems like Foundry and Gotham:

"So what we're looking at is the expansion of the use of Foundry across multiple state platforms and Palantir is very explicit about that being what they want to do. You know, they're very, Karp has said before, you know, our aim is to dominate institutions in the 2022 letter to shareholders. He said, we don't intend to capture part of the market, we aim to capture the whole. And their long term aim is for, you know, the majority of Western states operations to be running on that platform. And in the wider context of Palantir's encroachment into the state as a whole, Louis Mosley about a year ago in January 2025 argued that the UK government should adopt a common operating system that's able to link NHS data with Department of Work and Pensions data and other kind of public data sources on its

system. And he kind of, you know, unsurprisingly gave Foundry as an example of a software that would be able to do that."

These comments aren't buried in secret boardroom memos leaked by a whistleblower. These are statements made openly, on the record, to parliamentary committees, to public inquiries, in open letters to shareholders. Senior executives from Palantir standing before our government and calmly advocating for a common operating system across the British state, explaining interoperability, describing seamless data movement, making the case in plain English for why their infrastructure should sit at the heart of public services. And the most sobering part?

Our government is definitely listening and their response isn't resistance, it's procurement. Because make no mistake, they want what Palantir's systems can do.

Here's Rhiannon again:

"In 2017, the former head of NHS Digital kind of revealed that the Home Office was repeatedly demanding access to migrants' confidential health data without the proper legal frameworks. And so they had to backtrack on some of the data sharing, but there are still data sharing agreements in place."

Kingsley Manning, then chair of NHS Digital, later told Parliament he was put under quote: "immense pressure by the Home Office to release confidential patient data to assist immigration enforcement." He raised concerns about whether the Home Office even had a proper legal basis to access confidential patient records.

But the department's position, he said, was that it should be able to use that data for public policy purposes and that NHS Digital shouldn't be questioning that assumption too closely. At the same time, there was a formal Memorandum of Understanding in place between NHS Digital and the Home Office, allowing patient information to be disclosed for immigration-related tracing requests. In fact, the Home Office made up

the majority of requests handled under NHS Digital's National Back Office review.

Rhiannon: "The Home Office has wanted migrants' data, health data, for years and has like, has a little bit of it and is dying to get more. The UK government is in the context of massively wanting to expand their ability to police and deport people. And Palantir is a perfect partner for all of this, who now has access to huge amounts of health data as well. So it wouldn't take loads, you know some changes in legislation, some ignoring of legislation for a current or future government to say, okay, well, we're going to combine these data sources now and, you know, find the protesters we don't like and find the undocumented migrants we want to deport."

It's important to note that the arrangement between NHS Digital and the Home Office was formally ended in 2018 after legal challenge and parliamentary scrutiny. Since then, health data governance has been tightened under UK GDPR, the Data Protection Act 2018 and NHS England's Information Governance Framework.

The Federated Data Platform operates within those rules. Access is role-based, use is limited to defined purposes like direct care and operational planning, and formal safeguards are required before data is processed. On paper, the protections are clear. The NHS say the supplier of the platform was appointed in line with public contract regulations and must only operate under the instruction of the NHS, with all access to data remaining under NHS control and strict contractual obligations protecting confidentiality.

But for campaigners like Rhiannon, medical watchdogs like the BMA and of course us here at Good Law Project, there is a real fear that the protections are only as good as the paper they are written on.

Jo Maugham, Founder of Good Law Project: "Civil society groups are describing this as the repurposing of healthcare data for surveillance because it is the repurposing of healthcare data for surveillance. And you

know, it's happening in the United States and kind of weirdo conspiracy theorists are worrying that it might happen in the United Kingdom."

This is Jo Maugham, Founder of Good Law Project:

"Am I one of those weirdo UK conspiracy theorists? I am absolutely one of those UK weirdo conspiracy theorists. You know, it's absolutely right to say you can't just read across from what US law permits to what UK law permits. We have GDPR which provides various types of safeguarding for the use of data and those safeguards don't exist or don't exist in the same way in the United States. But I'm not much comforted by that right and here's why. First of all we are giving Palantir the means with which to do it and we are relying on it complying with the law in discarding the possibility that it will do it. So it can do it and it has to in essence voluntarily decide that it's going to be legally compliant and not do it. You know and I'm kind of suspicious right, I don't feel very comfortable with Palantir saying don't worry we won't do any of this; I just I don't feel that's a very reliable promise.

Secondly, when we were in the EU, it would have been very very difficult for us to change GDPR. Now we are outside the EU and it is very very easy for us to change GDPR. If you had a government that was bent on a mass deportation campaign and wanted to find out information about citizens that NHS doctors might hold, like who on your database is an adult but has only been in the NHS database for five years, let's say. It would be very, very easy for that new government bent on that mass deportation campaign to ask Palantir to answer that question with the names of all of the people fitting that category and then you'd have kind of a long list for deportation. You'd have a group that looked like they were recent arrivals to the United Kingdom.

And then you say to yourself, well, is there a possibility of a government wanting to embark on a mass deportation campaign? Well, not really even a possibility, right? Because Labour is starting to use that kind of language, the present government, and Reform, which is presently riding high in the opinion polls is making absolutely no secret of its desire to forcibly remove 550,000, 600,000 people in the first term. If the UK

GDPR is a bar to Reform doing that, do you think it will adhere to that bar or do you think it will just change GDPR? I mean, to me, the answer to that question is blindingly obvious. It will change UK GDPR.

As Tech and Data Lead at Good Law Project, Duncan McCann underlines:

"I think we have a Reform party that's actively talking about emulating a lot of what's going on in the US. We've seen them already in the councils that they've tried to appropriate the DOGE cost cutting measures. And I think with their stance on immigration, you know, they have already made noises about looking to mimic, copy, learn from what is happening in the US and what is going on with ICE.

And so I see again the coming together of a company willing to do whatever is necessary, whatever those in power want, coupled with a government in reform. But also, I think the other parties are also edging closer and closer to a kind of rhetoric around immigration and control. You see that with Labour with their ID cards and their digital surveillance. So I think Reform represents the sharp end of the risk, but I think it's a slow and general trend towards more data surveillance and more kind of oversight at that kind of technical level."

Palantir insists it complies with all laws and lawful data sharing agreements, adding that it's the customer, the government, that controls how data is used. But can we really rely on Palantir to operate strictly within UK law? Not just in principle, but in practice? If the FDP contracts were not renewed in 2027, can we be confident that any data processed within their systems would be fully and verifiably deleted, as contractually required?

Do we trust that they wouldn't make that data available to a foreign government or bad actor for the right price?

Jo Maugham: "Dealing with Palantir and expecting it to do the right thing is a bit like kind of asking a guy dressed in black and white hoops and carrying a bag marked 'Swag' to house it for you and relying on his good

faith assurances that he's not going to kind of walk off with any of your possessions. That's how I feel about it.

Palantir can be obliged to delete the data. But how can you ever know that Palantir actually has deleted the data? How do you know that it hasn't been copied onto a hard drive? You just, you can't know. Everything that we know about how key figures in Palantir see the world causes me, and I would say should cause all of us, to be deeply sceptical or at least closely inquisitive about whether Palantir really is going to do these things that we might be legally in a position to ask it to do, but have no way of checking whether it has actually done. You know it's a one-way street really, you hand this data over to Palantir and you can never know that you're going to get it back without Palantir keeping it."

You might argue that much of this is conjecture, doom prophecy and conspiracy theory. But as Jo explains, this is exactly the kind of prophetic modelling our government should be entertaining when considering bedfellows as problematic as Palantir.

Jo Maugham: "I'm a lawyer and I kind of think about this stuff as a lawyer does. So in climate change law, I think in public health law, there's this thing called The Precautionary Principle. And it says that if you're confronted with a risk of something happening, which is serious and irreversible, you should think very long and hard before you take that risk. And I think there's room to read The Precautionary Principle into how we deal with a company like Palantir, because we can't know that if we give it this data, it will be possible to reverse that decision.

Maybe we can take it on trust that under this government, Palantir won't use the data for unlawful purposes, but if we have a future government that is even more right wing than this one and it says to Palantir, did you guys hang on to that data that you should have deleted? It would be very convenient to us if you did. We might just discover that Palantir did what was convenient to do anticipating a further right wing government. So you can't give Palantir this stuff in a way that you can be confident is reversible. And I think we're kind of missing that really profound point in the way in which ministers and policymakers are dealing with a company

that it has every reason to think has really quite dark political objectives. The more we know about Palantir, the more we worry, maybe for a while it was mere suspicion that healthcare data in the United States would be used to target people for forcible removal from the United States and now we know that it's fact.

Surveys of healthcare providers across multiple US states show evidence of a chilling effect, where fear-linked immigration enforcement can deter people from seeking healthcare and other services.

And those fears, that lack of trust in a Palantir-powered healthcare system are already beginning to spread delicate cracks throughout our NHS.

Hope Worsdale: "You know, we work with patients who share things with their doctor that they don't even share with their family members."

This is Hope Worsdale, Head of Comms and Digital Impact at patient advocacy group Just Treatment:

"It's really vital that patients feel trust in the NHS and in their doctors and their GPs and in the information that they're sharing. Otherwise, it can impact how patients engage with healthcare. Patients need to feel that their data is being managed in a responsible and ethical way. And I think responsible and ethical are two words that probably most people would not associate with Palantir.

There are already examples of certain kinds of patients, particularly marginalised patients, not sharing fully their health problems with the NHS because they don't know how that's going to be used. So for example, certain migrant communities basically because there is now a kind of quite opaque system of sort of information sharing you know between the health service, between the Home Office...we know for a fact that there are already patients that are thinking I would actually just rather not be honest about my health or actually not even go to my doctor and not even engage with the NHS because I am fearful for how that information is going to be shared and how that information could be used against me.

That erosion of trust, it does have very real consequences for how people choose to engage with the health service. And for any public health service to function effectively the core thing that you need is patients to be able to like be honest with their clinicians and their GPs and their doctors, and share that information completely freely – knowing that you know it's not going to kind of in some way be used against them, or that it's not going to in some way be used for a purpose that they haven't consented to etc etc."

We don't yet have UK-wide data showing people have stopped using NHS services because of Palantir and the FDP specifically. It's too early and it's not being tracked in a clean way. But what is clear is that our trust is beginning to be eroded, fundamentally and perhaps permanently. Not just because of who Palantir is and what it does, but because of what our current and future governments might want it to do.

For many within the healthcare sector, and beyond, the case against Palantir lies in a fundamental ethical truth. How can a public health service founded on healing and the protection of life align itself with a company supplying advanced AI and data tools to military operations in Gaza, a campaign that has levelled hospitals and killed thousands of civilians?

Here's Rhiannon again:

"I think it's quite simple. Palantir are an extremely violent company involved in AI warfare, deportations, state surveillance and there's absolutely no way that a company like that should be involved with the health system.

The genocide in Gaza, in the very particular way in which the Israeli project targets the health of Palestinians, has been a real eye-opener for lots of health workers and has been a real moment of reckoning, of realising that as health workers, you cannot afford to be apolitical. You cannot afford to say: we don't have a stake in this system and our patients are just patients and they make the choices that they make and that's why they're healthy or not healthy. The ability for a health system to function,

the ability for health workers to adequately serve their patients and the ability for people to live lives of dignity is a political choice. And the genocide in Gaza couldn't have made that more clear."

Palantir claim they take a rigorous approach to respecting human rights from development to consumer use of our products. They also say they are very proud of the support they have provided to Israel.

When executives speak about dominating institutions, when interoperability between healthcare systems and military systems is framed as seamless, when the infrastructure that manages waiting lists can technically interface with the architecture used for battlefield intelligence, critics see not just efficiency, but concentration of power. And in political climates where rhetoric hardens around immigration, protest and national security, that concentration begins to look less like innovation and more like capability waiting for direction.

Technofascism isn't about today's safeguards. It's about what becomes possible tomorrow once the pipelines are laid. Because once data from health, welfare, policing and defence exists within interoperable systems, once that integration becomes routine, the gap between care and control is no longer hardline. It's an admin setting.

And when a public health service depends on absolute trust, the mere proximity of that infrastructure to enforcement logic can be enough to fracture confidence. You don't need tanks in the street to feel controlled by the system. You only need the right software and a government willing to ask it the right questions.

But here's the thing. For all the inevitability in the language, for all the glossy dashboards and ministerial enthusiasm, for all the talk of modernisation and momentum...this story isn't over.

In our next episode, we uncover the glimmer of hope in resistance. We'll reveal how NHS England's glowing uptake numbers are far less triumphant than their press releases might suggest. And how key figures within Trusts are beginning to speak out about the hidden costs and

glacial rollout of systems that in many cases don't even offer the functionality of the ones they are replacing.

We'll hear how local systems in hospital Trusts like Manchester and Cambridge are already showing that there is an alternative, that Palantir is not the only path to modernisation, not the only way to integrate data, not the only future on offer.

We'll look at how momentum is growing at every level both inside and outside the NHS, with clinicians, analysts, campaigners and patients organising, Trust by Trust, board by board and at grassroots level. To put pressure on our government to turn away from Palantir right at the time that their political baggage is coming back to haunt them.

From Peter Thiel's documented ties to Jeffrey Epstein, to Peter Manderson's consultancy's role in opening doors in Westminster, we'll see how these associations may become increasingly uncomfortable as scrutiny intensifies and Palantir's contract renewal in 2027 becomes anything but a foregone conclusion.

I'm Eliza Pitkin. Join me next time for episode 4 of the Shadow Contract. Signed, Sealed, but far from Delivered.

We put the concerns raised in this episode to Palantir. While they did not respond directly to our questions, they have made a number of public statements addressing these issues. They insist they are not and have never been a surveillance company, saying, quote: "we do not conduct surveillance, we do not provide surveillance services, nor do we sell our software for the purposes of enabling unlawful surveillance".

Important to note that this doesn't rule out lawful surveillance, or a future government that could change the law so Palantir could use NHS data. Palantir also insist that their engineers, quote: "are only able to access NHS data under the direction of the data controllers. This only takes place for appropriate engineering activities like data pipeline deployment and product support tasks. People in the institutions we serve can only see the information they need to in order to do their job and so that it is possible to see exactly who accesses what data, why and when."

Palantir points to comprehensive information outlining how data is processed within the FDP, published by the NHS, including the Information Governance Framework and Data Protection Impact Assessment.

If you're listening to this, it means you care about the truth. At Good Law Project, we don't just expose wrongdoing, we go to court to stop it. From secret NHS data deals, to PPE cronyism, to environmental destruction quietly signed off by the government, we uncover what's hidden, hold power to account and use the law to resist hate and bring hope. But here's the truth. We can only keep protecting you and exposing stories like this one if you stand with us. We don't take corporate money, we answer to no party or private interest. We're people powered. We're funded by people like you. Injustice is not inevitable. So if you believe in truth, accountability and the right to know what's being done in your name, support our work. Go to **goodlawproject.org/podcast** and give what you can. Because if we don't fight for transparency, who will?