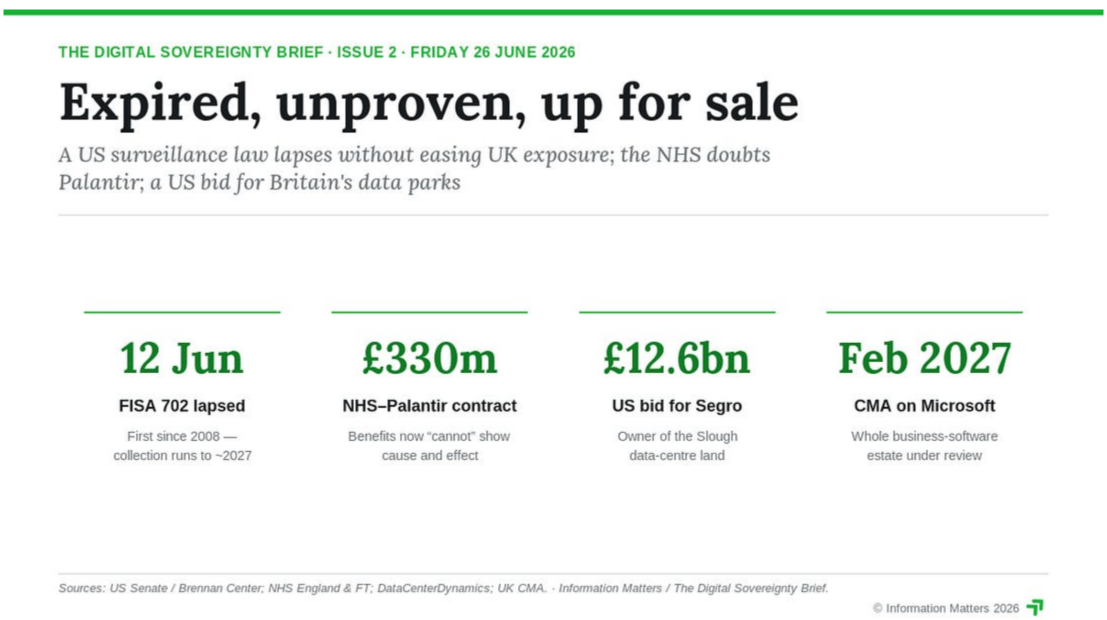
The Digital Sovereignty Brief #2 — Expired, unproven, up for sale

A US surveillance law expired without easing the exposure of UK data on American clouds; the NHS admitted it cannot prove Palantir works; a US landlord bid for Britain's data parks.

MARTIN DE SAULLES

JUN 25, 2026



Sovereignty watch — a US surveillance law expired, and your exposure did not. Section 702 of the US Foreign Intelligence Surveillance Act — the authority that lets US agencies collect data held by American providers without a warrant — lapsed at midnight on 12 June, the first time it has expired since 2008, after the Senate failed to advance reauthorisation on a 47–52 vote. A lapsed statute reads like good news for anyone whose data sits with Microsoft, Google or AWS. It is not. The Foreign Intelligence Surveillance Court renewed its annual collection certifications earlier in 2026, and those

> keep Section 702 collection running until roughly March 2027 regardless of the lapse.
>
> For UK organisations the practical position is unchanged: the legal basis on which a US agency can reach data held by a US provider still operates, it has simply moved from statute to court certification for the remainder of its run. Our verified Microsoft 365 assessment — which already rated the risk of a foreign authority lawfully reading UK data as high, driven by jurisdiction, not by where the data is stored — stands as it was. The date worth marking is the certification expiry around March 2027, or any reform bill that passes before then. Brennan Center, FISA 702 resource page · Roll Call on the 5 June vote

---

The week in six lines:

- **A surveillance law expired, and nothing eased.** Section 702 lapsed on 12 June, but court certifications keep US-government collection of data held by US providers running to about March 2027 — the exposure UK organisations carry on US clouds is the same as it was a fortnight ago.
- **The NHS conceded it cannot prove its US platform works.** NHS England now says its headline Palantir benefit figures "cannot draw conclusions about cause and effect," and FT analysis shows a third of trusts did fewer operations after adopting the scheduling tool.

- **A US landlord bid for the ground UK data sits on.** Prologis offered about £12.6bn for Segro, owner of the Slough data-centre land that hosts much of Britain's cloud capacity; Segro's board rejected it.
- **The CMA put all of Microsoft's software under the microscope.** A Strategic Market Status investigation now covers Windows, Office, Teams, Copilot and security software, with a designation decision due by February 2027.
- **Britain treated standards-setting as a sovereignty tool.** DSIT's new Digital Standards Strategy names AI, cyber, quantum and semiconductors as priorities and funds a national quantum-standards network; the Data Act's complaint-handling duty came into force.
- **The thread:** this week's sovereignty questions were domestic and concrete — who can lawfully read UK data, and who owns the systems and the land it runs on.

The through-line: the abstractions came home this week. The question of who can reach UK data, and who owns the infrastructure it depends on, was answered in a Senate vote, an NHS methodology page, a data-centre takeover bid and a competition probe — all of them about control that sits outside Britain.

Ownership & control

NHS England admits it cannot show that Palantir's platform caused the improvements it claims. NHS England has defended its £330m Federated Data Platform contract with the US firm Palantir by pointing to roughly 110,000 additional operations and a 15% fall in discharge delays. On the methodology page behind those numbers, the health service now states it cannot "draw conclusions about cause and effect as other variables have not been controlled for." An FT analysis found the gains lean heavily on a handful of hospitals — one trust, Chelsea and Westminster, accounts for 84% of the cited fall in outpatient waiting lists across the sixteen trusts using the platform — and that some trusts performed fewer operations after adopting the software than before. A cross-party group of MPs has called on ministers to trigger the 2027 break clause and seek a UK-based provider.

So what? the case for keeping a US-controlled supplier inside England's patient-data infrastructure has rested on measurable benefit, and NHS England has now qualified that benefit as causally unproven on its own page. Palantir is a Delaware company whose founder retains voting control and whose chief executive is an outspoken political actor; the contract holds records on tens of millions of people, and the break-clause decision falls before the independent evaluation NHS England has commissioned even reports. A dependency this deep is worth keeping only if it can be shown to work, and this week the people running it stopped claiming that it can. NHS England FDP methodology page · NHS England uptake and benefits · FT — Palantir NHS claims rely on just a few hospitals (paywalled)

And a separate question hangs over who can read the data. The government's own national data guardian, Nicola Byrne, has asked NHS officials to explain why they did not disclose that staff from companies including Palantir would have, in the words of an internal NHS England briefing note, "unlimited access" to identifiable patient information through a new "admin" role on one part of the platform. Byrne said she had been assured access would be limited to NHS staff with a legitimate need, and was unaware of any change of policy.

So what? the sovereignty of a health system is not only about who owns the contract but about who can lawfully see the records inside it. An access arrangement the data guardian was not told about goes to the heart of that, and it sharpens the break-clause question rather than softening it. FT — UK government adviser urges clarity on Palantir access to NHS patient data (paywalled) · NHS England response to the national data guardian

Data & infrastructure

A US landlord has bid for the ground much of Britain's cloud sits on. Prologis, a San Francisco-based real-estate investment trust, disclosed on 24 June an approach valuing Segro at about £12.6bn. Segro is the London-listed owner of the powered data-centre land clustered around Slough — the corridor through which a large share of UK hyperscaler and colocation capacity is physically delivered, with tenants including Amazon and Equinix. Segro's board rejected the offer as undervaluing the company, and Prologis has taken its case to shareholders.

So what? sovereignty arguments usually stop at the data and the software, but the physical estate underneath has an owner too. Moving Segro into a US REIT would place the land that hosts a meaningful portion of Britain's cloud capacity under American control, and would concentrate the physical layer further at a moment when the UK is trying to expand it. Land ownership is not the same as data jurisdiction, but a bid on this scale for this corridor is reviewable under the National Security and Investment Act, and is worth watching on those terms. DataCenterDynamics

Google says it will process some sovereign UK workloads in-country. At its London summit on 17 June, Google Cloud said its Gemini 3.5 Flash model would be available for UK sensitive and sovereign workloads with in-country processing by late June, alongside its Waltham Cross data centre and new public-sector deployments.

So what? "processed in the UK" answers where the work runs, not who can compel the company running it. Google remains a US provider within the reach of the same certification-based collection regime discussed above, wherever the rack sits, and the announcement does not say whether the model's weights, training and sub-processors are equally in-country. It is a useful procurement option to test, on its detail rather than its label. Google Cloud blog

Reports & analysis

A US export order is a sovereignty problem, not an AI-policy footnote. Writing for CEPR's VoxEU on 22 June, the researcher Marco Perugini argued that the 12 June US directive suspending access to Anthropic's models for non-US users exposed a structural gap: European — and by extension British — public infrastructure runs on US cloud with no institutional means to contest or delay such an order. He cites the Kiel Institute's estimate of around €500bn over a decade to close Europe's military-AI capability gaps, and notes, with a declared conflict of interest, that the column was drafted using the very system the order restricted.

So what? Britain is named in neither this column nor the European scenarios it draws on, yet sits in the same position — outside the EU's collective instruments and, as the Anthropic shutoff showed, outside any exemption arrangement with Washington. Treat the piece as argument rather than evidence, but the gap it describes is the one our framework keeps returning to: a tool you cannot keep running without another government's permission is a dependency, whatever its address. CEPR / VoxEU

Regulation & policy

The CMA has put Microsoft's whole software estate under formal scrutiny. The Competition and Markets Authority's Strategic Market Status investigation, under the Digital Markets, Competition and Consumers Act, covers Windows, Office, Teams, the Copilot and agentic-AI suite and security software. The consultation closed on 4 June with more than 130 responses; a statutory nine-month clock runs to a designation decision by February 2027. The named concerns include bundling, interoperability limits and whether AI competitors can plug into the ecosystem at all.

So what? every large UK public body — NHS trusts, HMRC, local authorities — runs on Microsoft, and our verified Microsoft 365 work treats the difficulty of switching away as a core part of the exposure. This is the first UK regulatory test of whether that lock-in can be loosened in the AI era; a designation would hand the CMA powers to impose the licensing and interoperability remedies its 2024 cloud inquiry said were holding switching back. A standing item to February 2027. CMA press release · CMA case page

Britain is treating standards-setting as an instrument of sovereignty. DSIT published its Digital Standards Strategy for 2026–2030 on 17 June, naming AI, cybersecurity, advanced connectivity, quantum and semiconductors as priority domains, committing to UK leadership in the international standards bodies, and funding a £10m national quantum-standards network led by the National Physical Laboratory. The document is explicit that some governments use technical standards to extend control over emerging technologies.

So what? standards are a quieter lever than compute spending and a more durable one — the body that writes the rule shapes how every product built to it is judged. Where the UK co-authors a standard, as the NCSC did on AI cybersecurity, it gains a say in how cloud-hosted AI is assessed for British procurement. It is one of the few sovereignty tools that costs little and compounds. DSIT Digital Standards Strategy — gov.uk

The Data Act's complaint-handling duty is now live, and adequacy is the thread. From 19 June, the Data (Use and Access) Act 2025 requires every data controller to run a formal complaints procedure and acknowledge complaints within 30 days — the last of the Act's staged commencements.

So what? the interest for sovereignty is not the mechanic but the foundation it sits on. The Act underpins the European Commission's renewal of UK data adequacy to the end of 2031, the legal basis for UK–EU data flows; a pattern of enforcement failures would become material in any future adequacy review. The complaints duty is a small piece of keeping that bridge standing. DUAA commencement plan — gov.uk

The EU's cloud-sovereignty law has moved into the fight phase. The European Commission's proposed Cloud and AI Development Act, part of the package covered in Issue 1, drew a sharp response from the industry group CCIA, which called its top sovereignty assurance levels — EU ownership, control and personnel requirements — "closed-market requirements dressed up as policy thresholds," and argued no major technology producer, the EU included, currently meets them.

So what? the Act's graduated assurance levels are a state-level version of the jurisdiction ladder our own profiles use. For Britain the hinge is its "associated country" mechanism, which could in principle let UK providers be treated as EU-equivalent — but only through further Commission legislation, and UK adequacy helps without guaranteeing it. CCIA speaks for the incumbents it would constrain, so read its reading of the text as a position, not a finding. Worth tracking as the European Parliament takes it up. CCIA Europe statement · EC Cloud and AI Development Act policy page

---

Coming up at Information Matters.

- **The cross-sector picture** — eighteen UK sectors profiled on the same framework, and the shared floor underneath them: the three US clouds, Microsoft, and the card schemes.
- **Government & public sector** — the profile that follows healthcare, on the systems running local and central government.

Thanks for reading The Digital Sovereignty Brief! Subscribe for free to receive new posts.

Subscribed