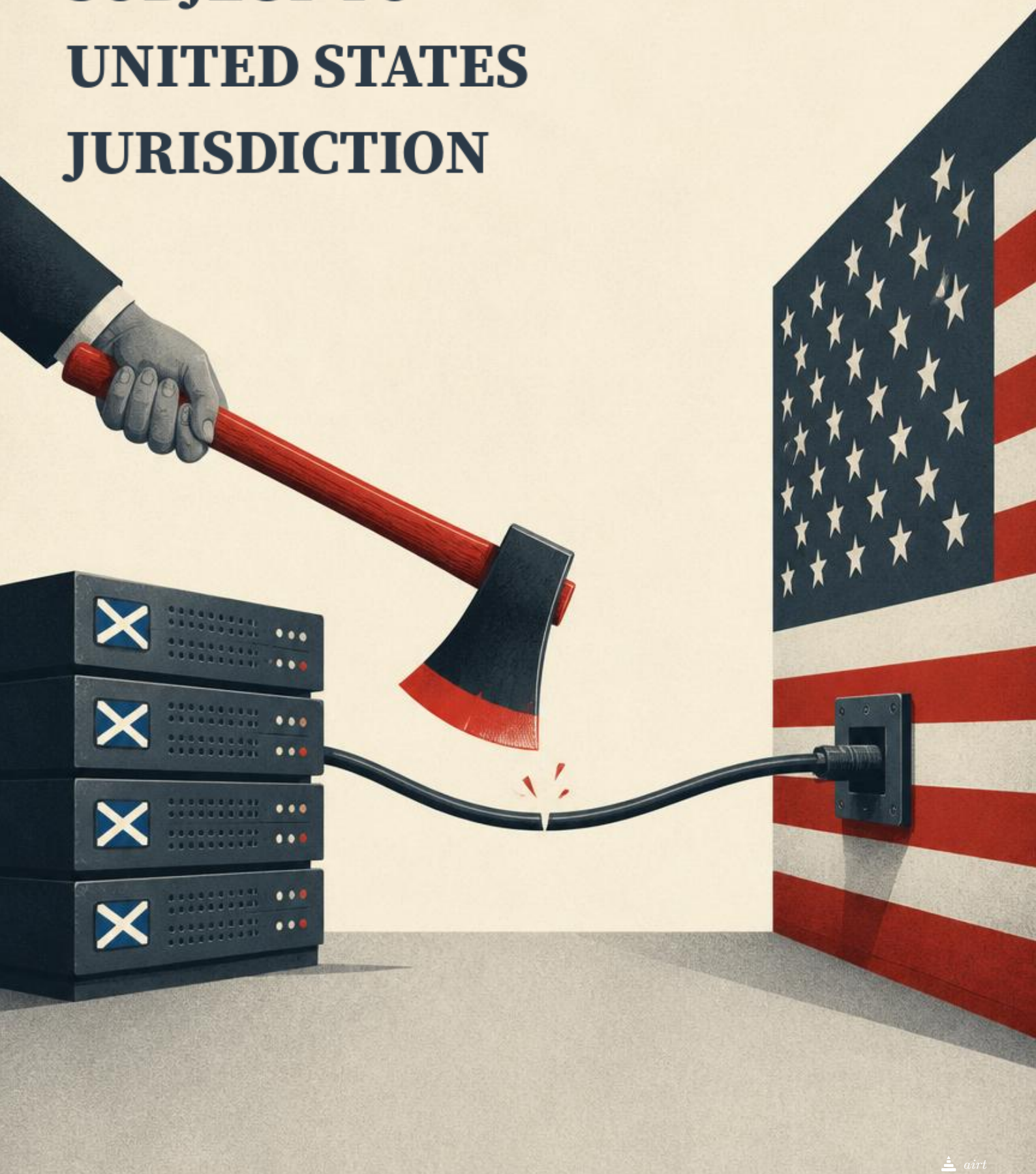
SUBJECT TO UNITED STATES JURISDICTION



June 2026

Subject to United States jurisdiction

An American company switched off its best software for every foreigner on earth one Friday evening, on a government order that named no reason, and complied while it was suing that same government in court. The machines under Scotland's health records, its digital identity and its government post answer to the same power. The Scottish Government's own files, released under freedom of information, show no record of assessing the risk, and no costed plan to leave.

The Friday switch

At 5:21 on a Friday evening in Washington, the American firm Anthropic received a letter from the United States government and did as it was told.[1] Within hours it had cut off its two most capable AI systems to every foreign national on earth, including the foreign nationals working in its own offices. The instrument was an export-control directive from the Commerce Department. It came wrapped in national-security language and named no specific concern. The software had been on sale that week. It was gone by the weekend.

The order had no half-measure. United States export law treats a foreign national's access to controlled technology, even on American soil, as an export to their home country, and you cannot geofence a foreign-born engineer at a desk in San Francisco. So "bar foreign nationals" collapsed into "pull the models for everyone," and Anthropic disabled both systems for every customer worldwide to comply at all.[2] The denial lever has no precision setting.

The software was the visible part. The lever is the transferable one. A company incorporated in the United States can be ordered, by a single stroke of executive power, to deny its service to foreigners, at no notice, on a Friday, for a reason that need not survive daylight. And it will comply. Anthropic was already at law with the same government in a separate matter, where weeks earlier a federal judge had blocked an attempt to bar federal agencies from using its technology, and it complied with the Friday order anyway.[3] Goodwill did not protect its foreign users. The jurisdiction did the deciding.

So, the plain question. What does Scotland run on?

[1] Anthropic, statement on the suspension of Fable 5 and Mythos 5, 12 June 2026 (anthropic.com/news/fable-mythos-access); Axios, "Trump admin blocks foreign access to Anthropic's most powerful AI," 12 June 2026; Fortune, 13 June 2026. The Commerce Department directive, signed by Secretary Howard Lutnick, issued at 5:21pm Eastern.

[2] Anthropic's own account of the "net effect": because US export law counts a foreign national's access as an export, and the firm cannot reliably separate foreign nationals from US persons across a userbase in the hundreds of millions, the only way to comply was a global shutoff of both models. See Just Security on the deemed-export mechanism, June 2026.

[3] The wider dispute: after the Department of Defense designated Anthropic a "supply-chain risk" and a federal directive ordered agencies to stop using its technology, Anthropic sued (9 March 2026) and a federal judge granted a preliminary injunction blocking the designation on 26 March 2026 (NPR, 26 March 2026). This is a separate lever from the June export control; both are instances of compelled denial.

What Scotland runs on

Over the past month I put that question to the Scottish state under freedom of information, system by system, and the answers point one way.

NHS Scotland's National Digital Platform, the shared spine of the health service's data, runs on Amazon Web Services under a ten-year contract from 2020, held in Amazon's London region. The Community Health Index, the register that holds a record for every patient in Scotland, runs on Microsoft Azure.[4] ScotAccount, the Scottish Government's own digital identity service, the one it wants you to use to prove who you are to government online, runs on Amazon.[5] So does the new Digital Mailbox, the channel through which it intends to send you official post; it was built through a CivTech challenge by the Danish firm Netcompany, resold through Computacenter, and deployed on the government's own Amazon platform.[6] Four foundations, all on American cloud.

The data centres really do sit in Britain, and that buys less than it looks. The point is law, not geography. An American company answers to Washington's courts wherever its servers happen to spin. The Scottish Government conceded exactly this in writing. Asked where ScotAccount runs, it replied that the provider is "Amazon Web Services (AWS), UK regions only," that the data "is processed and stored within the UK," and then, in the same breath and its own words, that "Amazon Web Services (AWS) is subject to United States jurisdiction."[7] That is not my phrase. It is theirs.

These particular providers are not neutral pipes either. In June 2025 a director of Microsoft France was asked, under oath before a committee of the French Senate, whether he could guarantee that data held for French public-sector customers would never be passed to American authorities without the French government's consent. His answer, in French, was four words: no, I cannot guarantee it.[8] Microsoft has spent years in court over the other half of the problem, the secrecy. It sued the United States Department of Justice in 2016 over gag orders that stopped it telling customers when the government had read their data, citing 2,576 secrecy demands in eighteen months, roughly two-thirds of them with no end date at all.[9] Compelled

[4] NHS National Services Scotland, from 1 April 2026 part of Public Services Delivery Scotland (PSD Scotland), FOI-2026-3367, response 5 June 2026: the National Digital Platform is hosted on Amazon Web Services under a ten-year contract commencing 2020 (1+3+3+3), London region only, with no data replicated outside the UK; the Community Health Index "is hosted in Microsoft Azure, not in AWS"; and PSD Scotland holds no exit plan or migration strategy, "as this area has not yet been decided" (s.17).

[5] Scottish Government, FOI 202600516387 (ScotAccount hosting), response 8 June 2026: "The cloud infrastructure provider is Amazon Web Services (AWS), UK regions only. The data for ScotAccount is processed and stored within the UK. Amazon Web Services (AWS) is subject to United States jurisdiction."

[6] Scottish Government, FOI 202600519882 (Digital Mailbox), response June 2026: the service is deployed within the government's AWS Cloud Platform Services, built under CivTech Challenge 9.8 (a Pre-Commercialisation Agreement with Netcompany UK plus a Call-Off through Computacenter UK as reseller); data residency specified as UK and/or EEA.

[7] Scottish Government, FOI 202600516387 (ScotAccount), as cited above.

[8] French Senate, commission of inquiry, 10 June 2025: Anton Carniaux, Director of Public and Legal Affairs, Microsoft France, asked under oath whether he could guarantee that French public-sector data would never be passed to US authorities without French consent, answered "Non, je ne peux pas le garantir" (reported by The Register and SDxCentral, 25 July 2025).

[9] Microsoft v. United States Department of Justice, filed 14 April 2016, US District Court for the Western District of Washington; Microsoft cited 2,576 secrecy demands over eighteen months, about 68% of them with no end date. The suit was dropped in October 2017 after the DOJ issued a policy curbing indefinite gag orders (Microsoft, "Keeping secrecy the exception, not the rule," 14 April 2016; blogs.microsoft.com/datalaw).

to hand the data over, and forbidden to say so. That is the documented record of one of the two companies Scotland's patient index sits on.

Disclosure and denial

That jurisdiction does not reach you one way. It can take the data, and it can switch off the service, and the difference between those is where the harder problem hides.

Taking the data runs through law. The CLOUD Act, passed by Congress in 2018, lets American law enforcement compel a US company to hand over data through a court order, wherever in the world that data sits.[10] This is the disclosure lever, the reach most data-protection arguments worry about, and the one providers answer with talk of encryption and customer-held keys. It has at least a shape: a statute behind it, a court order to point to, and a chance to contest it, the chance Microsoft took in 2016. But the right to contest belongs to the provider, not to the person the data describes. Your medical record can be handed over by a company in Seattle exercising, or choosing not to exercise, a right that is its own and never yours. The secrecy these orders carry means you may be the last to know, or never know at all.

Follow the incentives and the asymmetry gets worse. Resisting an order costs the provider: lawyers, delay, and friction with the government that signs its other contracts. The harm of complying falls on a data subject whose protection is the home authorities' job, not its own, and whom it cannot tell. An actor that pays to refuse and pays nothing to comply does not stop at the midpoint; the pull runs past compliance, toward handing over early and wide. Whether it crosses into overcompliance, more than the law strictly demands, is contested, and the firms insist they meet lawful orders and nothing beyond. You do not need the strong version. The only party that can contest the order, and then only if it is not gagged from doing so, has every reason not to, and you have no way to make it.

Switching off the service runs through nothing of the kind, as Anthropic demonstrated on a Friday. The executive can order the same company to go dark, by directive, in an evening, with no reason it has to give.[11] This is the denial lever. It takes your tool, not your data, and the usual reassurances do nothing against it. Encryption does not keep a service running. A customer-managed key does not turn it back on. The UK-US Data Access Agreement, offered as the grown-up channel for cross-border requests, governs how data is asked for and handed over; it says nothing about an order to stop serving you. Every one of those reassurances answers disclosure. On denial they are silent, and denial is the lever that just fired in public.

The non-answers

When I asked whether any of this had been weighed, the answer kept coming back no.

ScotAccount's data-protection assessment does not consider the CLOUD Act, and the Scottish Government says so as policy. A data-protection impact assessment, it told me, is "not

[10] Clarifying Lawful Overseas Use of Data Act (United States, 2018), which amended the Stored Communications Act so that a US warrant or court order for data reaches a US provider regardless of where the data is stored, and which set up the framework for executive agreements such as the UK-US Data Access Agreement.

[11] Anthropic suspension, 12 June 2026, as cited above.

intended to be a comprehensive assessment of international legal regimes that could theoretically apply to cloud suppliers"; it assesses against UK data-protection law, and so the CLOUD Act and the Data Access Agreement fall outside it by design.[12] The point is fair: a data-protection assessment may be the wrong place to look for jurisdictional risk. But the question was also put where it belongs. Asked whether it had assessed ScotAccount's continuity against a hosting provider being sanctioned, sold, or withdrawn, the government answered that it had found no risks "materially different from those managed for other digital services using public cloud infrastructure," and holds "no separate, ScotAccount specific document assessing these risks in isolation."[13] A provider switched off by its own government, or compelled to hand a foreign state your data, is being treated as no graver than an ordinary cloud outage. The jurisdiction question has not gone unasked by accident; it has been folded into routine cloud risk, where it stops being visible. The Digital Mailbox holds no recorded CLOUD Act assessment either, and no review under Article 35(11) of the UK GDPR of whether recent American demands for cloud-held data have changed the risk.[14] In none of what it disclosed had the danger been examined and judged small. In none of it had the danger been examined at all.

On leaving, the files say the same thing. There is no ScotAccount-specific exit or migration plan with a defined timeline or cost; only, in the response's own words, "high-level exit considerations" folded into "general governance."[15] The health platform and the patient index hold no exit plan either.[16] Four nation-scale systems on foreign cloud, and not one of them has a costed way back off it.

The scale is not small. ScotAccount held just over 768,000 registered accounts at the start of June 2026, and it processes biometric data, the special category the law guards most closely, to verify identity; the government notes the biometric images are deleted once the check is done.[17] This is the layer the state wants between you and every online service it runs, sitting on US-jurisdiction cloud, with the jurisdiction question ruled out of its own risk assessment.

The absence reaches below the headline platforms. myaccount, the older shared sign-in still used across Scottish local government, names all 32 councils as joint data controllers of the registration data. I asked one of them, Fife, the same questions I had put to the centre. Fife holds no data-processing agreement, no CLOUD Act assessment, no impact assessment addressing

[12] Scottish Government, FOI 202600516387, response 8 June 2026: "Data Protection Impact Assessments (DPIA) are not intended to be a comprehensive assessment of international legal regimes that could theoretically apply to cloud suppliers... the ScotAccount DPIA does not specifically identify and assess the risk of extraterritorial data access under the US CLOUD Act 2018 or the UK-US Data Access Agreement."

[13] Scottish Government, FOI 202600516387: asked whether it had assessed ScotAccount's continuity against a hosting provider subject to "international sanctions, ownership change, or service withdrawal," it replied that no such risks "materially different from those managed for other digital services using public cloud infrastructure" had been identified, and that it does "not hold a separate, ScotAccount specific document assessing these risks in isolation."

[14] Scottish Government, FOI 202600519882: no recorded assessment of the CLOUD Act in respect of the hosting provider or sub-processors (s.17), and no review under Article 35(11) of the UK GDPR of whether recent US-authority data demands change the risk (s.17, not held).

[15] Scottish Government, FOI 202600516387: "there is no ScotAccount specific plan that includes defined timelines or cost estimates," only "high-level exit considerations" as "part of general governance."

[16] NHS NSS / PSD Scotland, FOI-2026-3367, as cited above: no exit plan or migration strategy held (s.17).

[17] Scottish Government, FOI 202600516387: "At 1 June 2026 ScotAccount had just over 768,000 registered accounts"; the service processes Article 9 biometric special category data for identity verification, "fully deleted once the check is completed." For scale, GOV.UK One Login had passed 13 million identity-verified users by late 2025 (Government Digital Service) and was still climbing as HMRC and other services onboarded through early 2026.

compelled disclosure, no record of any continuity or hosting-jurisdiction correspondence, and no exit plan: six requests, six confirmations that nothing is held.[18] The one thing it could tell me was that the data sits "on servers within the UK," which, as the Scottish Government has already conceded about its own systems, is the answer to the wrong question.

A "not held" is an absence of records at the body asked, not proof the work was never done anywhere; the cross-service questions Fife could not answer would, on its own account, sit with the shared service that the councils buy in. I put a narrower version to the centre too, asking the Scottish Government for any impact assessment covering registration data shared across services. That one was refused on cost, and the specific assessment confirmed as not held.[19] So the pattern holds at both ends. The systems are live and growing, and at every door I knocked on the assessment was somewhere else, or nowhere.

Nobody switches off the NHS

That is the reassurance, and it deserves saying plainly because it is mostly true. No American president is going to reach across the Atlantic and turn off an intensive-care ward. The risk is not that one Friday the health service goes dark.

Why Friday's order was given is the alarming part. The fear officials pointed to was that the software was unusually good at finding flaws in other programs, even ones it was handed only as finished, compiled software with no source code attached: a cyber-weapon in waiting. The security researcher who reviewed the underlying work said it was close to the opposite of a weapon: the same capability is how defenders find and patch holes before hostile states reach them, and it "should never have triggered an export control."[20]

The concept is almost mundane. A program is just instructions acting on the input it is given, a flaw is a place where it trusts input it should not, and finding one means feeding it the malformed and the unexpected and watching for where it gives way. The skill, and the years, are in doing that well by hand; the machine's only new trick was doing it fast. It is the reverse engineer's day-job, shared by rival systems, a trade four decades old with tools anyone can download.[21]

[18] Fife Council, FOI FCIR 65137, response 16 June 2026: as a myaccount data controller, Fife confirmed it holds none of the requested items (data-processing agreement, CLOUD Act assessment, impact assessment on extraterritorial disclosure, jurisdictional-resilience correspondence, exit plan), each under s.17; the one positive answer was that "all data is held on servers within the UK."

[19] Scottish Government, FOI 202600516370 (cross-service registration data sharing), response June 2026: questions on scoping refused under s.12 (cost), and no data-protection impact assessment for cross-service registration data sharing held since 2020 (s.17, not held).

[20] Katie Moussouris (Luta Security) described the flagged capability as Defense Oriented Prompting rather than a jailbreak, and said it "should never have triggered an export control" (Fortune; TechCrunch, June 2026). Anthropic says the function is a limited code-review capability also present in rival models (it names OpenAI's GPT-5.5). The government's counter, put by White House adviser David Sacks, is that Anthropic was warned and declined to fix the flaw, alongside an unverified claim of China-linked access; Anthropic disputes both, and neither has been demonstrated publicly.

[21] The craft has its own literature. Phrack, the underground technical journal, has published on vulnerability research and exploitation since 1985 and reached its fortieth-anniversary issue (#72) in 2025; it sits alongside the deadpan PoC or GTFO journal and the USENIX Workshop on Offensive Technologies, with open decompilers such as Ghidra freely downloadable. Finding flaws in compiled software is a discipline with a forty-year paper trail, not a new capability.

The government's side, put by a White House adviser, is that Anthropic was warned and would not fix the flaw, and that a China-linked group may have reached the restricted model; the company disputes both, and neither has been shown in public.[22] What is not in dispute is that blocking one provider contained none of the capability, because it lives in a dozen other places.

That is the part that should travel. A rule you can predict, you can build around. An order whose stated reason dissolves on contact, you cannot. The exposure is not malice. Nobody in Washington is plotting against Scottish patients. The exposure is arbitrariness: an instrument that can be aimed at "foreign nationals" on a Friday evening, for a reason that need not hold up, by a government you do not elect and cannot petition. You are not depending on a regulator. You are depending on a mood.

A mood meets no limit until it meets something with teeth. The teeth here were meant to be American law, and on this record they had the form and not the bite. Anthropic won a court order against one instrument in March and was hit by another in June; it was suing the government throughout and complied anyway. Every state stretches the powers it grants itself; the question is whether its own checks can hold the line. Here they could not: block one instrument and the next one fires.

A frontier model is not a hosting contract

The fair objection to all of this is that I am comparing different things. Friday's pull was an export control on a frontier AI model. It was not a hosting contract, and Amazon did not switch off NHS Scotland's servers. That is true, and it matters.

The parallel is by mechanism, not by instrument. An AI model under export control and a hosting platform under the CLOUD Act sit under different laws, and the essay does not pretend otherwise. What the two share is the part a government planner should not wave away: United States executive reach over a United States company, used outside America's borders, at speed, with "foreign nationals" as the line it draws. Scotland's public bodies and the Scottish public are precisely that to a US-incorporated provider. Friday did not prove the NHS will be switched off. It proved the mechanism is real, fast, and indifferent to whether the provider objects, because the provider that complied within hours was suing the same government at the time.

Nor was Friday a one-off. The same reach has recurred since the start of the second Trump administration, across different instruments and not only against AI. After a US sanctions order in 2025, the Microsoft email of the International Criminal Court's chief prosecutor, in The Hague, was cut off and his bank account frozen; when Washington then weighed sanctions against the whole court, the threat to its entire Microsoft estate was credible enough that the ICC abandoned the company pre-emptively for a sovereign European suite.[23] In May 2026 Mi-

[22] Moussouris and the White House (Sacks) counter, as cited above.

[23] After President Trump's executive-order sanctions on the International Criminal Court's chief prosecutor, Karim Khan (6 February 2025), his Microsoft email was cut off and his bank account frozen; he moved to a Swiss email provider. In September 2025 Washington was reported to be weighing entity-wide sanctions on the Court, which would have compelled its US suppliers to cut it off; the ICC pre-emptively left Microsoft for openDesk, a sovereign open-source suite from Germany's Centre for Digital Sovereignty (ZenDiS). Microsoft's president disputes that it "suspended services" to the Court, saying it disconnected the individual account while keeping the ICC running. As reported (Computer Weekly; JusticeInfo; EJIL:Talk!; Reuters, 2025).

crosoft was reported to have handed a US congressional committee the internal data of Dutch regulators enforcing an EU law, their names unredacted.[24] Set those beside the Pentagon's attempt to bar Anthropic and the Commerce order that followed, and the picture is a run of instances, across sanctions, a legislative demand, procurement, and export control. The instruments differ, and so does the lever each pulls: disclosure in the Dutch case, denial in the others; what they share is the jurisdiction behind them. A single stray AI incident is not what the record shows, and neither is a clean line between models and hosting.

The two halves of the reach stand on different ground against Scotland's systems. The disclosure half needs no analogy: the CLOUD Act is written to compel hosted data, and the Dutch case shows it reaching an allied state's own regulators. The denial half is not pure inference either: the Hague case put the reach into hosted cloud and made a whole institution flee it. What the record does not yet show is that done at the scale of a nation's core platform. The gap is scale, not kind, and scale is no refuge. Until 17:21 on Friday there was no precedent for an export control seizing a frontier model either, one sold that week and already running worldwide through networks, hyperscalers, other firms and governments, in the most heavily guardrailed form its maker shipped. "No precedent" is the condition of every such act right up to its first occurrence, and Friday turned one of them into a fact. The reassurance that hosting sits in a safer category is the one that covered frontier AI on Thursday. It did not last the week.

The line between a model and a hosting contract is narrowing anyway. Most people picture AI as the chatbot they type at, or the clever trick that reads a number plate or folds a protein; in that picture the Anthropic affair stays safely over there, somebody else's problem. That is not where AI is heading. The hyperscalers that hold Scotland's data are folding AI into the platform itself, into the storage, the search, and the agents that move data about, and selling it not as a chatbot but as the operating system the rest runs on.[25] As that happens, the distinction this section just conceded begins to blur. The thing an evening's directive can reach stops being a product you could swap out and becomes part of the platform itself. The dismissal that a chatbot is not your hosting is fair today, and it has a shelf life. How long the line lasts is the open question; that it is being erased, and by the providers themselves, is not.

Governing it

None of this argues against digital public services, or against proving who you are once and getting on with your day. The convenience is real and worth having. It argues for governing the thing before it sets hard, while the contracts are still being signed and the dependence is still shallow enough to move.

[24] In May 2026 Microsoft was reported to have given a US House of Representatives committee examining the EU Digital Services Act internal data, including unredacted names, of Dutch officials at the consumer authority (ACM) and the data-protection authority (AP). As reported (NL Times; Cybernews, May 2026); coverage frames it as a US CLOUD Act-type exposure. Microsoft has not conceded the characterisation.

[25] By 2026 the major cloud providers present themselves not as raw infrastructure but as enterprise AI platforms, with foundation models, agents and orchestration built into the core services: Amazon's Bedrock is a managed model-and-agent layer inside AWS, with Microsoft and Google running the same vertical-integration play. The industry's own term for the destination is the "AI operating system" (Constellation Research and others, 2026).

The government could assess the exposure it admits it has not assessed, in writing and system by system, on the taking of data and the switching-off alike, instead of ruling the question out of scope. It could hold a plan to leave with a date and a cost against it, so the dependence is a choice and not a trap. And at the scale of a nation's health and identity it could require hosting that answers to Scottish or European law, with the resilience a serious state keeps for what it cannot afford to lose. Estonia, whose government runs on digital identity end to end, keeps a backup of its critical registers in a data embassy in Luxembourg, on sovereign Estonian ground abroad, so that no single jurisdiction holds the off switch.[26] Scotland has built the dependence and skipped the plan.

The capability was there on Thursday and gone by the weekend, for everyone outside one country and every foreigner inside it, switched off by the company that made it even as it fought the order in court. The machines under Scotland's health records and its identity layer answer to the power that threw that switch, and the files I was sent show no one planned for the day it reaches them. It was all theoretical, right up until 5:21 on a Friday evening.

Published on airt.scot. The freedom of information responses cited below are held in full; references and dates are given so the chain can be walked.

[26] A. Hardy (2024) on Estonia's X-Road, the once-only principle, and the data embassy in Luxembourg, where critical state registers are replicated on sovereign Estonian territory abroad.