IT'S STILL NOT CLEAR WHETHER ELON'S DOGE BOYS ARE REVIEWING, TAKING, OR ALTERING GOVERNMENT NETWORKS

The big news overnight in the legal fight to rein in DOGE is that SDNY Judge Paul Engelmayer has ordered Treasury to stop letting Elon Musk's DOGE [sic] boys to snoop in Treasury's payment system and *destroy* any copies of records already made from it. [docket]

> the defendants are (i) restrained from granting access to any Treasury Department payment record, payment systems, or any other data systems maintained by the Treasury Department containing personally identifiable information and/or confidential financial information of payees, other than to civil servants with a need for access to perform their job duties within the Bureau of Fiscal Services who have passed all background checks and security clearances and taken all information security training called for in federal statutes and Treasury Department regulations; (ii) restrained from granting access to all political appointees, special government employees, and government employees detailed from an agency outside the Treasury Department, to any Treasury Department payment record, payment systems, or any other data systems maintained by the Treasury Department containing personally identifiable information and/or confidential financial information of payees; and (iii) ordered to direct any person

> prohibited above from having access to such information, records and systems but who has had access to such information, records, and systems since January 20, 2025, to immediately destroy any and all copies of material downloaded from the Treasury Department's records and systems, if any;

This order comes on top of Judge Colleen Kollar-Kotelly's order limiting access to Treasury's payment system to normal employees and two DOGE [sic] employees, but the latter for read-only access [docket]:

> Mr. Tom Krause, a Special Government Employee in the Department of the Treasury, as needed for the performance of his duties, provided that such access to payment records will be "read only";
>
> Mr. Marko Elez, a Special Government Employee in the Department of the Treasury, as needed for the performance of his duties, provided that such access to payment records will be "read only";

Anna Bower parsed how DOJ substantiated (or not) that this was really "read only" access. Which was part of what a bunch of Democratic Attorneys General, led by Tish James, pointed to to claim they still needed a TRO, over and above the one issued by Kollar-Kotelly.

> The temporary restraining order entered yesterday by the D.C. District Court in Alliance for Retired Americans v. Bessent, No. 1:25-cv-313 (D.D.C.) ("ARA"), does not change this conclusion. That order continues to permit two SGEs affiliated with DOGE to have access to the BFS payment records and payment systems, restricts their access to "read only" just for payment records and not payment systems, and

> does not direct that any copies of data from the systems made since the Agency Action took effect be destroyed. ARA, Dkt No. 13.

Now, I'm somewhat skeptical that Engelmeyer's order, *as issued*, is sustainable. He issued the order in advance of the assigned judge on the case, Jeannette Vargas, and before the government had a chance to respond to the lawsuit.

But the lawsuits to enjoin DOGE [sic] are playing catch-up to the known facts.

And the known facts get us much closer to the being able to prove that Elon and his DOGE [sic] boys are altering code, if not hacking it, rather than simply reviewing its data.

The suit and TRO before Judge Kollar-Kotelly, filed by several unions, is entirely privacy focused.

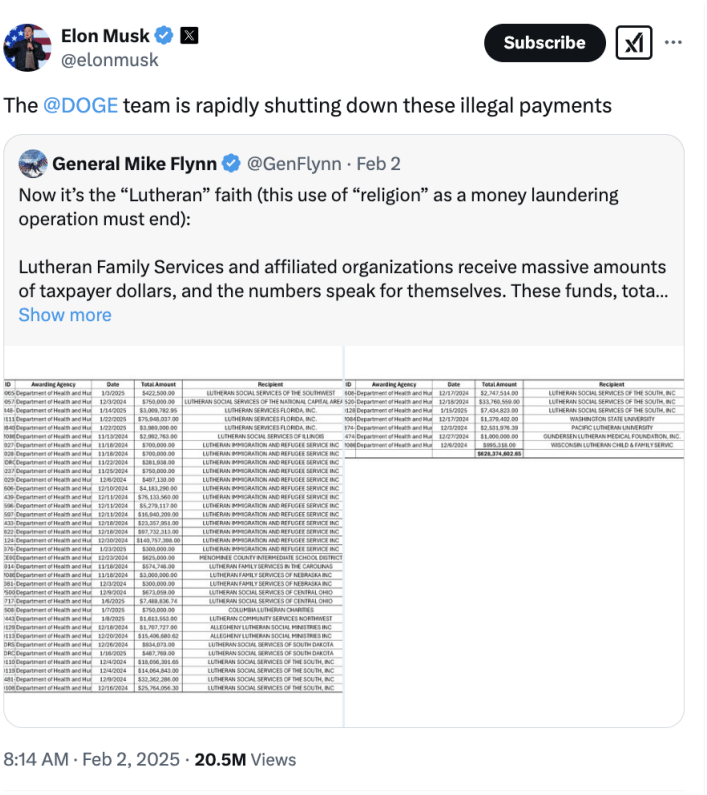
The state AGs' suit and TRO, which establish standing by pointing to the billions of dollars of payments they get from the Feds, argues that Elon is attempting to intercept payments to entities Trump doesn't like. It asserts a claim repeatedly backed in public reporting, but affirmatively denied before Kollar-Kotelly: that the DOGE boys — here, self-proclaimed eugenicist Mark Elez, *have altered code*.

> 5. As of February 2, 2025, the President and Treasury Secretary, directed Treasury to grant expanded access to BFS payment systems to political appointees and "special government employees" for reasons that have yet to be provided, although one apparent purpose, upon information and belief. Upon information and belief, one purpose is to allow DOGE to advance a stated goal to block federal funds from reaching beneficiaries who do not align with the President's political agenda. For example, DOGE was tasked with freezing

> payments issued by the U.S. Agency for International Development (“USAID”) and sought access to BFS payment systems to accomplish that goal.5 Virtually unfettered access to BFS payment systems was granted to at least one 25-year-old DOGE associate, Mark Elez, who, on information and belief, had the authority to view or modify numerous critical files.6 Indeed, reports indicate that Elez had administrative privileges over the BFS payment system’s code, giving him the ability to alter user permissions and “read and write” code—even if the associate had “read-only” access to the system’s data.7 Elez has since resigned from DOGE after being linked to racist social media posts.8
>
> 6. Around the same time that DOGE associates were unlawfully granted access to BFS systems, Mr. Musk began publicly stating his intention to recklessly freeze streams of federal funding without warning. On February 2, 2024, Mr. Musk posted on X (formerly Twitter), an online social media platform, that DOGE is “rapidly shutting down” various “illegal payments” made by the government to grant recipients, including payments to Lutheran Family Services to provide services to migrant children.9 That same day, Mr. Musk posted that his team “spent the weekend feeding USAID into the wood chipper.” Since then, Mr. Musk has unambiguously called for the cancellation of various streams of federal funding. For instance, on February 6, 2025, he alleged: “Billions of taxpayer dollars to known FRAUDULENT entities are STILL being APPROVED by Treasury. This needs to STOP NOW!”10 Mr. Musk has also made wild, unsubstantiated claims about the BFS payment system and suggested putting it on the blockchain.11

> 6 A 25-Year-Old With Elon Musk Ties Has Direct Access to the Federal Payment System | WIRED
>
> 7 https://www.wired.com/story/elon-musk-associate-bfs-federal-payment-system/
>
> 8 DOGE Staffer Resigns Over Racist Posts
>
> 9 Elon Musk on X: “The @DOGE team is rapidly shutting down these illegal payments” / X
>
> 10 Elon Musk on X: “Billions of taxpayer dollars to known FRAUDULENT entities are STILL being APPROVED by Treasury. This needs to STOP NOW!” / X
>
> 11 Fatima Hussein, “Elon Musk’s task force has gained access to sensitive Treasury payment systems, sources say,” PBS News, Feb. 2, 2025, https://www.pbs.org/newshour/politics/elon-musks-task-force-hasgained-access-to-sensitive-treasury-payment-systems-sources-say; Billy Bambrough, “‘This Needs To Stop Now’—Elon Musk Confirms Radical Doge U.S. Treasury Plan,” Forbes, Feb. 2, 2025, https://www.forbes.com/sites/digital-assets/2025/02/02/this-needs-to-stop-now-elon-musk-confirmsradical-doge-us-treasury-plan/.

It cites Elon’s insane rants on Xitter as well.



In addition to the privacy concerns addressed in the union lawsuit, the AGs' lawsuit raises concerns about appropriations (and separation of powers), but also cybersecurity, something not included in the union lawsuit.

> 139. The conduct of DOGE members presents a unique security risk to States and State residents whose data is held by BFS, given that **DOGE employees have already reportedly set up an unauthorized commercial server at another federal agency without a privacy impact assessment** as required by the 2002 E-Government Act. Access by DOGE employees to BFS is likely to present even greater risks to the security and privacy of States' and their residents' data.
>
> 140. Unsecure data is susceptible to cyber attacks and identity theft. Identity theft has a significant impact on States, beyond the financial well-being of its residents. It strains law enforcement resources, damages state economies through lost productivity and

> consumer confidence, and raises costs for the state to redress fraudulent claims made from stolen identities for unemployment and healthcare benefits. [my emphasis]

The AGs' suit actually doesn't cite a source for the claim that DOGE set up a commercial server at another agency. But I think the claim comes from a lawsuit Kel McClanahan filed against Office of Personnel Management, aiming to require it to stop the all-government email DOGE [sic] set up to offer its "Fork in the Road" severance offer. McClanahan first sued, with two plaintiffs who worked at government agencies, on January 27, for a violation of the E-Government Act. [docket]

In response, the government claimed that the main theory of injury, that the government had set up the all-government email without first doing a privacy assessment didn't apply for employees, and was moot because it had since done one, which it included here. The privacy assessment claimed this was just a Office365 account.

> 1.3. Has a system security plan been completed for the information system(s) supporting the project? The Office 365 mailbox has been granted an Authorization to Operate (ATO) that includes a system security plan. The government computer storing the data is subject to standard security requirements, including limited PIV access.

And it claimed that the account included only *employee* data.

> 2.1. Identify the information the project collects, uses, disseminates, or maintains. GWES collects, maintains, and uses the names and government email addresses of federal government

> employees. GWES also collects and redistributes responses to emails sent to those addresses, which are limited to short, voluntary, non-identifying information. Specifically, GWES contains the following:
>
> - *Employee Contact Data: GWES collects, maintains, and uses the names and government email addresses of federal government employees. Other identifying information is not used.*
> - *Employee Response Data: After an email is sent using Employee Contact Data, GWES collects, maintains, and redistributes short, voluntary responses.*

It largely ignored McClenahan's claim (based largely on Reddit posts) that DOGE had installed a separate server.

> But other than speculation on social media, Plaintiffs provide no evidence that OPM took any of the actions that would trigger the PIA requirement under sections 208(b)(1)(A)(i)-(ii) of the E-Government Act. Moreover, Plaintiffs disregard entirely the fact that the E-Government Act does not require a PIA when an agency is seeking to collect information about "agencies, instrumentalities, or employees of the Federal Government."

Since then, McClanahan filed an amended

complaint, which added five more plaintiffs, none of whom are Executive Branch employees (for example, one works for the Library of Congress; another is a contractor), substantiating that some of the DOGE emails went to people outside the Executive Branch, and provided additional substantiation of the Reddit claims (including raising questions about whether this could even be Microsoft365).

> 30. Furthermore, prior to 20 January 2025, OPM lacked the technical capacity to send direct communications to all Executive Branch employees: But just days before President Donald Trump's inauguration, OPM did not have the capability to send a mass email of that scale, according to a person familiar with the matter. To send mass emails, the agency had used govDelivery, a cloud communications service provided by public sector IT company Granicus, a different person familiar said. The govDelivery contract had restrictions on the volume of emails available to send without incurring added costs, and the agency would not have been able to reach 2.3 million people, the approximate number of all civilian federal employees, the second person added. David DiMolfetta, OPM's new email system sparks questions about cyber compliance Nextgov/FCW (Jan. 28, 2025), available at https://www.nextgov.com/digitalgovernment/2025/01/opms-new-email-system-sparks-questions-about-cybercompliance/402555/ (last accessed Feb. 3, 2025).
>
> 31. Additionally, OPM has used Microsoft Office 365 since at least 2021, including Outlook 365 for email. OPM, Privacy Impact Assessment for OPM – Microsoft Office 365 (May 13, 2021), available at https://www.opm.gov/information-management/privacy-

policy/privacypolicy/office-365-pia.pdf (last accessed Feb. 3, 2025). Outlook 365 cannot send more than ten thousand emails per day. See Microsoft, Exchange Online limits (Dec. 11, 2024), at https://learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-servicedescription/exchange-online-limits#sending-limits-1 (last accessed Feb. 3, 2025).

32. According to the FedNews Message, "Instead [of using the normal channels], an on-prem (on-site) email server was setup [sic]. Someone literally walked into our building and plugged in an email server to our network to make it appear that emails were coming from OPM. It's been the one sending those various 'test' message[s] [discussed below]." FedNews Message.

33. This statement is supported by recent reporting:

> A new server being used to control these [OPM] databases has been placed in a conference room that Musk's team is using as their command center, according to an OPM staffer. The staffer described the server as a piece of commercial hardware they believed was not obtained through the proper federal procurement process.

Caleb Ecarma & Judd Legum, Musk associates given unfettered access to private data of government employees Musk Watch (Feb. 3, 2025), at https://www.muskwatch.com/p/muskassociates-given-unfettered (last accessed Feb. 3, 2025).

34. Upon information and belief, this server and/or other systems linked to it are retaining information about every individual with a Government email

> address.

The amended complaint argues that the privacy impact was factually and legally insufficient.

> 39. Neither Biasini nor Hogan were OPM employees prior to 20 January.
>
> 40. Biasini worked at the Boring Company prior to 20 January. It is not currently known if he still works there.
>
> 41. Hogan worked at Comma.ai prior to 20 January. It is not currently known if he still works there.
>
> 42. The GWES PIA was both factually inaccurate and legally inadequate.
>
> [snip]
>
> 54. Upon information and belief, OPM has not ensured review of a PIA for any of these systems by any legally sufficient Chief Information Officer or equivalent official.
>
> 55. OPM has not published a legally sufficient PIA or made such an assessment available for public inspection for any of these systems.

In other words, as these twin lawsuits against Treasury get closer to arguing that Elon is not *looking for savings* but instead *altering the payment system*, McClanahan continues to chase proof that Elon's DOGE [sic] boys have added their own server which, by dint of sending emails to everyone (including people not employed by the Executive branch) with a .gov address, is collecting information on everyone *with* a .gov address.

Meanwhile, several other developments get closer to showing that Elon is hacking the government, not assessing it.

First, late this week, OPM removed access by some DOGE [sic] boys to more sensitive OPM

systems.

> Directives from the agency's interim leadership issued late this week indicated that DOGE representatives should be withdrawn from two principal systems containing personally identifiable information for millions of federal employees, according to communications reviewed by The Post and people familiar with the developments who spoke on the condition of anonymity because of the matter's sensitivity.
>
> Those systems are called Enterprise Human Resources Integration and Electronic Official Personnel Folder. They hold sensitive information about employees of most federal agencies, including addresses, demographic profiles, salary details and disciplinary histories.
>
> The Post reported Thursday morning that DOGE agents had gained access to those systems along with "administrative" access to OPM computer systems. That allowed them sweeping authority to install and modify software on government-supplied equipment and, according to two OPM officials, to alter internal documentation of their own activities.

Meanwhile, both Wired and WaPo have stories describing how a Booz Allen analyst described the DOGE [sic] access as an ""unprecedented insider threat risk;" the analyst was promptly fired.

> The review, delivered Monday to Treasury officials by a contractor that runs a threat intelligence center for Treasury's Bureau of the Fiscal Service, said that DOGE's access to the payment network should be "immediately" suspended. It also urged Treasury to

> scour the payments system for any changes approved by affiliates of DOGE, which is overseen by billionaire Elon Musk, the correspondence shows. DOGE stands for Department of Government Efficiency.
>
> A Treasury employee told The Post that the threat center is run by Booz Allen Hamilton, a large federal contractor. The company confirmed it runs the threat center, which it said is embedded within Treasury.
>
> Late Friday, after this article appeared, Booz Allen said it had "removed" a subcontractor who wrote the warning and would seek to retract or amend it. "The draft report was prepared by a subcontractor to Booz Allen and contained unauthorized personal opinions that are not factual or consistent with our standards," company spokesperson Jessica Klenk said. Booz Allen won more than $1 billion in multiyear U.S. government contracts last year.
>
> In a separate communication a week ago, a high-ranking career official at Treasury also raised the issue of risks from DOGE access in a memo to Treasury Secretary Scott Bessent, including the potential breach of information that could lead to exposure of U.S. spies abroad, according to five people with knowledge of the matter, who spoke on the condition of anonymity to reflect government deliberations. The memo included recommendations to mitigate risks, which Bessent approved, said another person familiar with the matter, who also spoke on the condition of anonymity.

And while the focus at Treasury has been on eugenicist Marko Elez, whom Elon has pushed to be reinstated, closer scrutiny into Edward "Big

Balls" Coristine — who is at OPM and possibly HHS — has described he has ties to hackers. Brian Krebs, who was targeted by some people in that crowd, described screen shots that suggest Coristine may have been fired for leaking internal documents to a competitor.

> *Wired* noted that Coristine only worked at Path for a few months in 2022, but the story didn't mention why his tenure was so short. A screenshot shared on the website pathtruths.com includes a snippet of conversations in June 2022 between Path employees discussing Coristine's firing.
>
> According to that record, Path founder Marshal Webb dismissed Coristine for leaking internal documents to a competitor. Not long after Coristine's termination, someone leaked an abundance of internal Path documents and conversations. Among other things, those chats revealed that one of Path's technicians was a Canadian man named **Curtis Gervais** who was convicted in 2017 of perpetrating dozens of swatting attacks and fake bomb threats — including at least two attempts against our home in 2014.

And Krebs provides chatlogs showing some of Coristine's former associates are taking notice.

> The Com is the English-language cybercriminal hacking equivalent of a violent street gang. KrebsOnSecurity has published numerous stories detailing how feuds within the community periodically spill over into real-world violence.
>
> When Coristine's name surfaced in *Wired*'s report this week, members of The Com immediately took notice. In the following segment from a February 5, 2025 chat in a Com-affiliated hosting provider, members criticized Rivage's

> skills, and discussed harassing his family and notifying authorities about incriminating accusations that may or may not be true.

Bloomberg matched Krebs' reporting on the reason for Coristine's firing from Path.

> "Edward has been terminated for leaking internal information to the competitors," said a June 2022 message from an executive of the firm, Path Network, which was seen by Bloomberg News. "This is unacceptable and there is zero tolerance for this."
>
> A spokesperson for the Arizona-based hosting and data-security firm said Thursday: "I can confirm that Edward Coristine's brief contract was terminated after the conclusion of an internal investigation into the leaking of proprietary company information that coincided with his tenure."
>
> Afterward, Coristine wrote that he'd retained access to the cybersecurity company's computers, though he said he hadn't taken advantage of it.
>
> "I had access to every single machine," he wrote on Discord in late 2022, weeks after he was dismissed from Path Network, according to messages seen by Bloomberg. Posting under the name "Rivage," which six people who know him said was his alias, Coristine said he could have wiped Path's customer-supporting servers if he'd wished. He added, "I never exploited it because it's just not me."

Bloomberg tied Coristine's past even more closely to organized abuse campaigns.

> JoeyCrafter was a member of Telegram groups called "Kiwi Farms Christmas

> Chat" and "Kiwi Farms 100% Real No Fake No Virus," both referencing an online forum known for harassment campaigns. Typically, the site has been used to share the personal information of a target, encouraging others to harass them online, in-person, over the phone or by falsely alerting police to a violent crime or active shooter incident at their home.

This is the kind of DOGE boy Elon has thrown at government networks — and thus far, Republicans don't seem to give a damn that Trump has given these DOGE [sic] boys access to data on virtually all Americans, employee or no.

One thing is clear, however: There's not a shred of evidence these boys are doing what Elon claims they're doing.

Most of these new facts — the seeming proof that OPM isn't doing what it claimed, the insider threat warning, the ties to hackers — are not in the AGs' suit. And by the time the suits catch up to the facts, the complaints may look quite different.

Update: Corrected that none of the OPM plaintiffs are employees of US Courts (though they did get an email).