

# JUSTICE KETANJI BROWN JACKSON TOLD YOU SO, SOCIAL SECURITY EDITION

The most important line in a court filing filed last week that disclosed DOGE was doing far more with Social Security data than then Social Security Administrator Leland Dudek claimed they were in a declaration submitted last March 24 reads, “SSA first learned about this agreement during a review unrelated to this case in November 2025.” (Docket) That, plus this discussion in the opening paragraph, is the only explanation for why the Social Security Administration (SSA) is just finding all this data now.

Based on its review of records obtained during or after October 2025, SSA identified communications, use of data, and other actions by the then-SSA DOGE Team that were potentially outside of SSA policy and/or noncompliant with the District Court’s March 20, 2025, temporary restraining order (“TRO”) (ECF 48). SSA notified the undersigned Department of Justice (“DOJ”) attorneys on December 10, 2025, of its concerns.

Something else led SSA to review DOGE access in October.

And while Debra Katz, the attorney for Social Security whistleblower Chuck Borges, claimed vindication from the disclosure, it’s not entirely clear whether Borges’ disclosures precipitated the discovery. He first came forward in August, two months before SSA appears to have started doing a real assessment of access violations, though he filed a retaliation supplement to his complaint in November.

Importantly, while Borges’ disclosures covered

the revelations in last week's filing, the most horrific of his disclosures pertained to actions that long post-date what is described in the filing, which all happened in March.

Last week's declaration revealed the following:

On *March 3, 2025*, a DOGE boy sent an email with an encrypted file to DHS, copying Steven Davis (who then was the operational leader of DOGE) and a DOGE boy formally assigned to Department of Labor. SSA has not been able to break the encryption and so don't know which 1,000 people the emailed records exposed.

The email attached an encrypted and password-protected file that SSA believes contained SSA data. Despite ongoing efforts by SSA's Chief Information Office, SSA has been unable to access the file to determine exactly what it contained. From the explanation of the attached file in the email body and based on what SSA had approved to be released to DHS, SSA believes that the encrypted attachment contained PII derived from SSA systems of record, including names and addresses of approximately 1,000 people.

From *March 7 through 17*, the DOGE boys were sending links *through* Cloudflare, and SSA has not bothered to ask Cloudflare what got sent or whether it still has the data.

[B]eginning March 7, 2025, and continuing until March 17 (approximately one week before the TRO was entered), members of SSA's DOGE Team were using links to share data through the third-party server "Cloudflare." Cloudflare is not approved for storing SSA data and when used in this manner is outside SSA's security protocols. SSA did not know, until its recent review, that DOGE Team members were using Cloudflare during this period. Because Cloudflare

is a third-party entity, SSA has not been able to determine exactly what data were shared to Cloudflare or whether the data still exist on the server.

Contrary to a declaration submitted by Mike Russo *on March 12*, the DOGE boys had more access than he disclosed at the time.

- a. Three DOGE Team members were granted access to a system containing SSA employee records for agency personnel for workforce initiatives.
- b. Two DOGE Team members were granted access to a system containing personnel access information to ensure terminated employees were unable to badge into the building or to access IT systems with their PIVs.
- c. Six DOGE Team members were granted access to shared workspace that would have allowed DOGE Team members to share data to which the employees had separately been granted access for fraud or analytics reviews.
- d. Two DOGE Team members had access to a data visualization tool that could connect to other data sources, which could provide access to PII.
- e. Two DOGE Team members had access to additional EDW schemas beyond those reported as of March 12, 2025.

*On March 24* (after Russo's declaration claimed all DOGE was doing was pursuing waste, fraud, and abuse), a DOGE boy signed a Data Agreement with a partisan group attempting to overturn some elections.

[A] political advocacy group contacted two members of SSA's DOGE Team with a request to analyze state voter rolls that the advocacy group had acquired. The advocacy group's stated aim was to

find evidence of voter fraud and to overturn election results in certain States.<sup>1</sup> In connection with these communications, one of the DOGE team members signed a “Voter Data Agreement,” in his capacity as an SSA employee, with the advocacy group. He sent the executed agreement to the advocacy group on March 24, 2025 ... but SSA has not yet seen evidence that SSA data were shared with the advocacy group.

*From March 26 (two days after the Temporary Restraining Order in question) until April 2, a DOGE boy had access to “ten EDW schema containing” Personally Identifiable Information, but the DOGE boy never used it.*

Contrary to some reporting and even more responses to the reporting on this, these abuses are *not* the most alarming things Borges disclosed, though they are *consistent* with parts of his whistleblower complaint. In truth, they provide details that make Borges’ earlier disclosures more concerning, such as that in the period when DOGE was sending data through Cloudflare, certain DOGE boys had just asked for and gotten access to the analytical warehouse, EDW.

First, around March 14, 2025, DOGE members requested access to PSNAP and SNAP MI databases for Payton Rehling and Aram Moghaddassi. Information reported to Mr. Borges indicates that proper approval through the Systems Access Management (SAM) system was bypassed for this request, which resulted in four user profiles.<sup>35</sup> The Security Access Management process requires a written request for data access that is then either approved or disapproved by a supervisor who provides a written justification for their decision. This process is necessary for oversight of database access approvals.

Additionally, these profiles concerningly included equipment pin access and write access. 36 Equipment pin access means that instead of a user accessing data through a personal pin identifier, which would make the accessor's actions traceable to a user, an equipment pin is used to verify the identity of a device or piece of equipment before it is granted access to a network or sensitive resources, potentially avoiding the creation of a record tied to a specific user. Giving a user "write access" means that the user will have the ability to edit data.

Granting access to databases that exceed authorized permissions violates the principle of least privilege, which holds that users should have the least amount of access necessary to do their job.<sup>37</sup> Information provided to Mr. Borges indicates that on Monday March 17, 2025, the EDW team discovered that users had been given access to data that was reportedly not authorized through normal approval channels.<sup>38</sup>

34 An Enterprise Data Warehouse (EDW) is a central, secure system that integrates data from various sources across an organization to support informed decision-making and strategic analysis. It acts as a single source of truth, providing a consistent and reliable view of data for reporting, analytics, and business intelligence.

35 Exhibit 1, p. 5

36 Exhibit 1, p. 5

But these disclosures are entirely separate from Borges' disclosures about what DOGE did after SCOTUS lifted the TR0 in June, which is that in August – so five months after the abuses disclosed last week – SSA DOGE boys including Ed

“Big Balls” Coristine with his ties to criminal hackers, created *an entire copy* of the SSA database and moved it onto a cloud not protected by government infrastructure.

The fact that DOGE was sending things via Cloudflare before that (and that SSA claims to be helpless to determine what got sent) demonstrates the danger of this. But it does not, remotely, address the danger.

As I said in August, when SCOTUS overturned Judge Ellen Lipton Hollander’s TRO in June, Justice Ketanji Brown Jackson warned about the skewed harm analysis SCOTUS was adopting.

Just last week, I wrote about the requirements for granting stay applications and, in particular, how this Court’s emergency-docket practices were decoupling from the traditional harm-reduction justification for equitable stays. See *Noem*, 605 U. S., at \_\_\_\_ (slip op., at 5). With today’s decision, it seems as if the Court has truly lost its moorings. It interferes with the lower courts’ informed and equitable assessment of how the SSA’s data is best accessed during the course of this litigation, and it does so without any showing by the Government that it will actually suffer concrete or irreparable harm from having to comply with the District Court’s order.

[snip]

Stepping back to take a birds-eye view of the stay request before us, the Government’s failure to demonstrate harm should mean that the general equity balance tips decisively against granting a stay. See *Noem*, 605 U. S., at \_\_\_\_ (slip op., at 4). On the one hand, there is a repository of millions of Americans’ legally protected, highly sensitive information that—if improperly handled or disseminated—risks causing

significant harm, as Congress has already recognized. On the other, there is the Government's desire to ditch the usual protocols for accessing that data, before the courts have even determined whether DOGE's access is lawful. In the first bucket, there is also the state of federal law, which enshrines privacy protections, and the President's constitutional obligation to faithfully execute the laws Congress has passed. This makes it not at all clear that it is in the public's interest for the SSA to give DOGE staffers unfettered access to all Americans' non-anonymized data before its entitlement to such access has been established, especially when the SSA's own employees have long been subject to restrictions meant to protect the American people.

We're only finding out about these earlier, less abusive violations, because lawyers and long-replaced SSA officials made declarations that have been debunked.

We're not finding out why SSA launched the review in October or November (though the notice reveals, "A review of the SSA DOGE Team's actions is ongoing"), and we're not finding out what they have learned about the more serious violations.