



LEGAL UPDATES

Federal “Information Silos” Protect Privacy – A New Executive Order Threatens Them

04/01/2025 | 4 minute read

On March 20, President Trump signed an Executive Order titled Stopping Waste, Fraud, and Abuse by Eliminating Information Silos, which calls for federal officials “to have full and prompt access to all unclassified agency records, data, software systems, and information technology systems...for purposes of pursuing Administration priorities related to the identification and elimination of waste, fraud, and abuse..., [including] authorizing and facilitating both the intra- and inter-agency sharing and consolidation of unclassified agency records.”

The temporary Department of Governmental Efficiency (DOGE) is seeking access to the sum of unclassified records held by the federal government, raising concerns among citizens and businesses alike.

Why This Matters

This Executive Order gives DOGE access to sensitive business tax information. Since 1976, federal corporate tax returns are confidential and protected from public disclosure under section 6103 of the Internal Revenue Code (IRC). Section 6103(a) states that officers or employees of the federal government may not disseminate the contents of business tax returns for unauthorized purposes without the taxpayer’s consent. Access to the returns of corporations, limited liability partnerships and other business entities is generally limited to certain government employees for tax administration purposes, other agencies pursuing a non-tax criminal investigation or persons with a material interest. (*See, e.g., Petitt v. Exigency Healthcare Servs., LLC*, No. 21-cv-07639-VKD, 2023 WL 2940181 (N.D. Cal. Mar. 10, 2023) (granting application to seal material that contained “confidential information[,] such as bank statements, ... tax statements[,] and supporting profit/loss documentation”))

The Executive Order allows for erosion of individual privacy, a cornerstone of our freedom. The Privacy Act of 1974 generally prohibits a government agency from sharing personal information without written consent, or another agency’s demonstrable need to know. In sponsoring the Privacy Act, Senator Sam Ervin (D-NC) explained why government access to our personal data must be limited and apportioned carefully among agencies:

Related People

Tedrick A. Housh, III,
CIPP/US, CIPP/E

Partner

Kansas City

816.460.5642

tedrick.housh@lathropgpm.com

Related Services

[Navigating the Second Trump Administration: Executive Orders & the Changing Legal Landscape](#)

[Data Privacy & Cybersecurity Compliance](#)

If we have learned anything in this last year of Watergate, it is that there must be limits upon what the Government can know about each of its citizens. Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words. (Legislative History of the Privacy Act of 1974, pg. 4.)

As amended by the 1988 Computer Matching and Privacy Protection Act, the Privacy Act specifies the narrow purposes under which an agency may share, receive and compare identifiable, individual-level data for matching. There is an established process for those seeking agency records containing personal information. Agencies must maintain proper accounting of any disclosures, including publication of a System of Records Notice (SORN). To allow for public comment, SORNs are published for 30 days before data can be accessed or shared in new ways. It appears that agencies have not been publishing SORNs before giving access to DOGE.

Who Needs to Know?

Everyone. We should be able to find out who in government has access to our sensitive and personal information, and why. In more than a dozen lawsuits brought under the Privacy Act, the rationale and limits of DOGE's data collection is being tested.

On March 20, the U.S. District Court for the District of Maryland temporarily enjoined the Social Security Administration (SSA) from continuing to give DOGE access to its treasure trove of personal information, including SSNs, medical and mental health records, driver's license information, bank account data, tax information, earnings history, birth and marriage records, home and work addresses, school records, immigration and/or naturalization records, health care providers' contact information, family court records, and employment and employer records.

In granting the TRO, the district court held that DOGE failed to establish a specific need for the data. A general desire to find waste, fraud and abuse fell short of the mark:

Defendants clearly understand why guarding privacy, rather than waiting for harm to occur, is important. After all, that is precisely the reason why they have withheld even the names of the members of the SSA DOGE Team. But, defendants have not shown the same level of care with the far more sensitive, confidential data of millions of Americans who entrusted their government with their personal and private information. The trust appears to have been violated, without any articulated need. (American Federation of State, County and Municipal Employees, AFL-CIO, et al. v. Social Security Administration, et al.)

One of these cases will soon reach the appellate courts.

Across administrations, there have been persistent questions about the authority of the President to act unilaterally through Executive Orders. A federal district court in North Dakota recently described the "disheveled hodgepodge of law surrounding administrative agencies and executive orders," and then explained the reasoning behind separation of powers:

Presidents rely on the Constitution and the laws of the United States, then leave it to the courts to decide which ones give them power. The Constitution separated the powers of government for very good reasons. The separation of powers doctrine is not an esoteric point of procedure that academics make a fuss about to get tenure. After centuries, we as Americans do not understand what it was like to live under a monarchy without checks and balances. People fought to separate these powers in a new form [of] government. People died for this new government because they saw what happened when all the power was held in one hand. Power can be taken by force, given, or lost inch by inch. It is the job of Congress to enact the law. It is the job of the President to enforce the law. It is the job of the Judiciary to determine the boundaries of the law. (*Iowa v. Council on Env't Quality*, No. 1:24-CV-00089, 2025 WL 598928, at *23 (D.N.D. Feb. 3, 2025))



Until DOGE expires on July 4, 2026, all three branches of government will need to engage in determining the limits of its authority.

What You Can Do

Be cognizant of DOGE's potential access to your confidential, sensitive or personal information. Revisit your cybersecurity planning, in case the data accessed by DOGE is hacked or inadvertently disclosed to the public.

Pay attention to the court cases dealing with access to individual personal information held by the federal government – they will have a pronounced impact on the private sector and the future federal regulation of privacy. We are monitoring the legal challenges to the administration's actions related to data privacy and will provide updates. In the meantime, if you have questions about the impact of this Executive Order, please contact [Tedrick Housh](#) or your regular Lathrop GPM attorney.