University of Wyoming | College of Law
Firearms Research Center

Paper No. 2026-5
May 13, 2026
Student Working Paper

Congress Banned a Gun Registry; AI Inference May Render the Prohibition Obsolete

Del Schlangen[*]

Federal law prohibits the establishment of "any system of registration of firearms, firearms owners, or firearms transactions" under 18 U.S.C. § 926(a). The existing debate over that prohibition has focused on whether ATF's digitization of out-of-business dealer records violates § 926(a). This paper argues that the debate, as framed today, overlooks a more consequential question: whether modern Artificial Intelligence (AI) inference capabilities could derive registry-equivalent knowledge from lawfully held federal data without the construction of a formal registry at all; and whether a current administration policy directive calling for the ingestion of "all government data" into AI models puts that possibility on a collision course with the statute.

Drawing on Professor Daniel Solove's framework treating AI-generated inferences as functionally equivalent to collected data, Professor Orin Kerr's mosaic theory of aggregated surveillance, the Supreme Court's ruling in Carpenter v. United States (2018), and the chilling-effect jurisprudence in Lamont v. Postmaster General *(1965) and* NAACP v. Alabama *(1958), this paper contends that § 926(a)'s prohibition was not designed to address the inferential capabilities that machine learning now enables. The paper examines the shift in federal AI governance from the Biden administration's risk-evaluation framework to the current administration's push to accelerate AI deployment, finding that neither approach has*

[*] J.D., 2026, University of Denver Sturm College of Law (anticipated); Master of Public Policy, 2019, American Military University; B.S., 2016, George Mason University, *cum laude*.

engaged with the specific legal tension between broad data ingestion and the firearms registry prohibition.

Key legal issues raised in this paper include the interpretation of § 926(a) given emerging AI inference capabilities; the effect of the Supreme Court's decision in Loper Bright Enterprises v. Raimondo (2024) on future challenges to ATF's data practices; the lack of AI-specific governance at ATF regardless of administration; and the potential chilling effect on Second Amendment rights that is posed by the growing capacity to infer firearms ownership utilizing AI. A review of the existing literature on these subjects identified no law review article, policy paper, or legal brief addressing this intersection directly. This paper seeks to fill that gap.

Introduction

Michael Kratsios, the Director of the White House Office of Science and Technology Policy (OSTP) stood in front of a room of national security professionals at the Center for Strategic and International Studies (CSIS) in July 2025 and outlined in broad terms the Trump administration's vision for artificial intelligence (AI) in the government:

> Over time, the way that these essentially models will operate on a government level is [that] all the government data that a government has is going to be ingested into models to provide citizen services. Whether it's the way you pay your taxes, whether it's your health care records, whether it's small things like if you want to apply to, you know, get a permit to go to national park for a campsite – all of this stuff is going to be part of – part of the AI fabric.[1]

Director Kratsios's remarks are best understood as a summation of the administration's strategic direction and not a self-executing legal mandate. The relevant question is whether that direction has been or will be operationalized via administrative action such as executive orders, OMB memoranda, agency acquisitions, and interagency data-sharing agreements. As this paper will demonstrate, and as the trajectory of federal AI policy since this speech shows, the answer is yes. The Genesis Mission Executive Order, issued in November 2025, formalized AI-accelerated integration of federal scientific datasets as official policy and established institutional infrastructure that could be extended to other agencies and their data, including law enforcement records as the policy matures.[2]

[1] CTR. FOR STRATEGIC & INT'L STUDIES, *Unpacking the White House AI Action Plan with OSTP Director Michael Kratsios* (July 30, 2025) (transcript), https://www.csis.org/analysis/unpacking-white-house-ai-action-plan-ostp-director-michael-kratsios.
[2] Exec. Order No. 14363, 90 Fed. Reg. 55,035 (Nov. 24, 2025).

The vision is ambitious from a technological perspective, but it also highlights an important, and largely unexamined, tension with existing federal firearms law. That's because the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) currently holds at least 920.7 million (henceforth rounded to 921 million) digitized firearm transaction records.[3] And in 1986, Congress looked at the possibility of the federal government compiling firearms ownership data and enacted an express prohibition, the Firearm Owners Protection Act.[4]

That prohibition is codified as 18 U.S.C. § 926(a).[5] It prohibits the establishment of "any system of registration of firearms, firearms owners, or firearms transactions." Not a "searchable database", not "a comprehensive list." Any system.

Director Kratsios did not mention the ATF and did not explicitly discuss firearms data of any kind during his articulation of administration policy. But ATF is a federal agency, and its records are government data. The policy path he described, subsequently formalized through executive orders and OMB directives, did not include a carve-out for records subject to existing statutory access prohibitions.

At some point, the policy framework for AI ingestion of "all the government data" and the existing statute prohibiting "any system of registration" are likely to come into direct tension. The question is whether we address this tension proactively or reactively.

I. The Contemporary Registry Debate

The question of whether ATF's current digitization practices constitute a firearms registry prohibited by law is not a new debate. Gun rights organizations have argued for years that ATF's digitization and centralization of out-of-business dealer records constitutes a prohibited registry under 18 U.S.C. § 926(a).[6] ATF has maintained that it does not.[7] The debate has catalyzed congressional investigations, proposed legislation, and extensive public commentary.[8]

---

[3] Jordan B. Cohen, CONG. RSCH. SERV., IF12057, *Statutory Federal Gun Registry Prohibitions and ATF Record Retention Requirements* (Feb. 5, 2024).
[4] Firearms Owners' Protection Act, Pub. L. No. 99-308, 100 Stat. 449 (1986) (codified as amended in scattered sections of 18 U.S.C.).
[5] 18 U.S.C. § 926.
[6] Aidan Johnston, *ATF Has Nearly 1 Billion Records in a Registry*, GUN OWNERS OF AM. (Jan. 31, 2022), https://www.gunowners.org/onebillionrecords.
[7] U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-552, *Firearms Data: ATF Did Not Always Comply with the Appropriations Act Restriction and Should Better Adhere to Its Policies* (2016).
[8] Press Release, Sen. Jim Risch, *Risch, Cloud Introduce Bill to Block Federal Gun Registry* (Jan. 16, 2025), https://www.risch.senate.gov/public/index.cfm/2025/1.

The legal questions surrounding this debate are genuinely contested. Does centralizing out-of-business firearms records make those same records an illegal registry? Does the act of digitizing paper records change their legal status? And does the ability to search within the documents materially matter, and if so, what degree or form violates § 926(a)?

The factual basis of the current debate can be further explained as follows. ATF by law stores records from firearms dealers who have either gone out of business or surrendered their licenses.[9] As of November 2021, the date of last available numbers, that number stood at nearly 921 million records, with 94% digitized into the Out-of-Business Records Imaging System (OBRIS).[10] The National Tracing Center within the ATF processes about seven million pages of gun sale records every month.[11] Given the passage of time since 2021 and the estimated monthly totals (seven million), the current total almost certainly exceeds one billion.

The ATF's position is that these digitized records don't constitute a registry because they're not searchable by purchaser name. In March 2024, then-ATF Director Steven Dettelbach explained: [12]

> I'm the only customer, ATF is of Adobe Acrobat, we pay somebody to take out search function, to remove search function that other customers have to in order to comply with the congressional notion that there can't be a gun registry in the United States.

The legal implications of the former director's statement deserve closer examination. ATF is acknowledging that it possesses all the underlying data, so every name, address, and serial number is visually present in the digitized files. ATF is also stating that it's legal position rests on the claim that the software feature allowing text-based search has been disabled. The data exists. The ability to search for it is, by the agency's own admission, a configuration setting away.

---

[9] 27 C.F.R. § 478.127 (2025).
[10] Cohen, *supra* note 3.
[11] Simone Weichselbaum et al., *'It's Just Insanity': ATF Now Needs 2 Weeks to Perform a Routine Gun Trace*, NBC NEWS (Aug. 19, 2022), https://www.nbcnews.com/news/s-just-insanity-atf-now-needs-2-weeks-perform-routine-gun-trace-rcna39606.
[12] *Face the Nation* (CBS television broadcast Mar. 3, 2024) (transcript available at https://www.cbsnews.com/news/steven-dettelbach-bureau-of-alcohol-tobacco-and-firearms-director-face-the-nation-transcript-03-03-2024/); NRA INST. FOR LEGIS. ACTION, *Face the Nation Airs ATF Propaganda*, NRA-ILA (Mar. 11, 2024), https://www.nraila.org/articles/20240311/face-the-nation-airs-atf-propaganda.

In fairness to ATF, the PDF nonsearchability claim is not its entire legal position, only the most visible layer. ATF's retention of out-of-business records is grounded in explicit statutory authorization, 18 U.S.C. § 923(g)(4), which requires that when a licensed dealer goes out of business, the dealer's required records "shall be delivered to the Attorney General" within a thirty day period.[13] The implementing regulation, 27 C.F.R. § 478.127, instructs these records to then be forwarded to ATF Out-of-Business Records Center.[14] ATF, therefore, maintains these records not as a result of any discretionary authority but through a congressional mandate. ATF's stated reason for retention, to assist in firearms tracing under § 923(g)(7), requires licensees to respond to trace requests within twenty-four hours and has been viewed as a legitimate law enforcement function.[15] Additionally, a permanent appropriations rider enacted in late 2011 forbids the use of federal funds to "electronically retrieve information gathered pursuant to 18 U.S.C. 923(g)(4) by name or any personal identification code."[16] ATF's legal position then, properly stated, is that it holds these records under a statutory mandate, retains them to perform a legally authorized tracing function, and does not retrieve them in a way forbidden or prohibited by Congress.

It is not disputed here that ATF has the statutory authority to possess out-of-business records or in contention that firearms tracing is a legitimate, legally authorized function. The argument advanced here is entirely different: that the lawful possession of data for one authorized statutory purpose does not implicate or solve the question of whether the computational transformation of that same data through inference into person-to-firearm ownership outputs violates a separate statutory prohibition.

The current debate, focused on what ATF has built or how it stores the data it lawfully holds, entirely misses an emerging technological question: whether AI inference capabilities makes building and maintaining a full-fledged, key-word searchable registry unnecessary to achieve registry-equivalent knowledge. The assumption at the heart of this debate, that a registry is something an agency like ATF builds and maintains, may no longer hold true in an era of advanced machine learning (ML).

[13] 18 U.S.C. § 923(g)(4).
[14] 27 C.F.R. § 478.127 (2025).
[15] 18 U.S.C. § 923(g)(7); Nat'l Rifle Ass'n v. Reno, 216 F.3d 122, 137 (D.C. Cir. 2000) (recognizing the legitimate law enforcement purpose).
[16] Consolidated and Further Continuing Appropriations Act, 2012, Pub. L. No. 112-55, div. B, tit. II, 125 Stat. 552, 609–10 (2011).

II. AI Inference and the Limits of Existing Statutory Protections

Daniel Solove's law review article "Artificial Intelligence and Privacy," published in 2025, provides a useful analytical lens for understanding how AI inference may upend the legal landscape around firearms data.[17] He states:

> Inference blurs the line between data processing and collection, which allows it to evade data collection limitations and other protections in many privacy laws.

This creates an issue for federal statutes anchored in data collection, such as § 926(a) and the Privacy Act of 1974. Privacy statutes, and by extension the firearms registry ban, typically regulate the affirmative actions of both storage and collection. They assume that the government's acquisition of knowledge about its citizens requires affirmative collection of that knowledge and that the information must be gathered and stored in some recognizable form. AI inference disrupts that assumption. Through inference, accurate information about individuals can be derived from existing datasets without an additional act of collection in the traditional sense. The government can effectively acquire information about a person it never affirmatively sought to collect.

Solove's normative conclusion on inference is straightforward: "the law should treat data derived from inferences on an equal footing with collected data."

Solove warns that AI's generation of data through inference creates "end-runs around privacy protections," producing information that current legal frameworks explicitly prohibit collecting. This observation maps precisely to the risk that AI inference poses to the registry prohibition at § 926(a). Congress prohibited collecting this knowledge in registry form. AI inference could generate its equivalent anyway.

Applied in the firearms context, the consequences are apparent. 18 U.S.C. § 926(a) prohibits "any system of registration."[18] The drafters of the 1986 law were thinking about contemporary data architectures, databases, physical filing cabinets, and mainframe queries. The primary question Congress sought to answer was whether the federal government could search its records for a citizen's name and identify the firearms they own.[19]

---

[17] *See generally* Daniel J. Solove, *Artificial Intelligence and Privacy*, 77 FLA. L. REV. 1 (2025).
[18] 18 U.S.C. § 926.
[19] S. Rep. No. 98-583, at 17–18 (1984), (stating that OOB records provisions were "intended to reassure law-abiding gun owners that such records will not become part of a centralized record system or system of registration").

AI inference poses a different question: whether the government can obtain "registry-equivalent" firearms determinations about individuals or groups without directly collecting, storing, and centralizing that data.

This paper utilizes the term "registry-equivalent knowledge" to describe a government capability that produces, via computation, the same types of identifying associations between individuals and firearms that a traditional registry would possess. The term and concept contain three distinct capabilities, each of which implicates § 926(a) to varying degrees. The first and most directly related capability to a traditional registry is the *individual-query capability*, or the ability to type in a person's name or other personally identifiable information and receive as an output a probabilistic determination of the firearms that person owns or has obtained. The second is *population-enumeration capability*, or the ability to create a list of probable firearms owners within a geographically bound area, demographic information, or other population subsets. The third is *reverse-trace capability*, or the capability to relate a specific firearm, identified by serial number, make, model, or ballistic signature, to a likely owner, without utilizing ATF's existing manual trace process. A system capable of demonstrating any one of these three capabilities through AI inference on federal data has produced the functional equivalent of what § 926(a) prohibits, even if no single database carrying the label "registry" exists. A system that achieves all three is, for all practical purposes, a de facto, or shadow registry. The analysis that follows does not assert that any of these capabilities have been operationalized or are in use today. It contends that the data, methods, and policy trajectory needed for operationalization are converging.

A "registry equivalent" determination via any one of these capabilities would not require a database field explicitly labeled "gun owner: yes/no." It would only require the aggregation and correlation of small bits of data already held across federal servers, things like transaction timestamps from specific licensed dealers, National Instant Criminal Background Check System (NICS) background check patterns, geographic proximity to ballistic evidence recovery sites, and Multiple Sales Report flags. With these disparate bits of information or others like it, AI could then be directed to derive specific and accurate associations about an individual or group's firearms ownership. Individual-query capability, as an example, could materialize from entity resolution across OBRIS images and eTrace records tied to a common name and address. Population-enumeration capability could be produced by gathering transaction records geographically in combination with demographic inference. Reverse-trace capability could be expedited by training a model on the existing eTrace dataset to predict ownership chains from serial-number and dealer-history inputs.

Today, these datasets are siloed into separate systems and databases, subject to different rules, access controls, and legal frameworks. This institutional separation serves as a

safeguard against the ability to create a de facto or shadow AI-inferred registry. However, the announced policy of ingesting all government data into AI models threatens to dissolve those safeguards and silos. The deliberate building of a cross-referencing system is unnecessary if the model has already ingested the constituent inputs.

It's a matter of debate whether any of these datasets in isolation would meet the statutory definition of a registry. Together, however, processed through modern machine learning, they could produce registry-equivalent knowledge.

This isn't a new concern in Fourth Amendment jurisprudence. Professor Orin Kerr's "Mosaic Theory," argues that aggregated surveillance can implicate constitutional concerns even when each individual act of surveillance does not.[20] The whole becomes greater than the sum of its parts. A single data point by itself carries little analytical significance. A billion data points subjected to computational analysis present an entirely different constitutional issue. Kerr's framework is doctrinal, not statutory, but conceptually, the logic applies in the same way that singular acts of location tracking may not be a search, but continuous and aggregated tracking is, individual federal datasets or datapoints may not constitute a registry, but their aggregated computational integration can produce registry-equivalent knowledge.

While no Supreme Court majority to date has adopted the mosaic theory explicitly as a doctrinal test, the Court's holding in *Carpenter v. United States* adopted the essence of its reasoning without invoking its name.[21] In *Carpenter*, the Court held that the government's attainment of past cell-site location information constituted a "search" requiring a warrant under the Fourth Amendment, despite each individual cell-site record, by itself, revealing little.[22] From a constitutional perspective, the concern arose from the aggregation of data points: 127 days of time-stamped location information produced what the Court called "detailed, encyclopedic, and effortlessly compiled" knowledge a person's movements, associations, and habits.[23] The Court specifically cautioned that legal rules "must take account of more sophisticated systems that are already in use or in development" and refused the argument that "inference insulates a search."[24]

[20] *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).
[21] 585 U.S. 296 (2018); *see also* Orin S. Kerr, *Implementing Carpenter* (Dec. 14, 2018) (unpublished manuscript), https://ssrn.com/abstract=3301257.
[22] *Carpenter*, 585 U.S. at 310–11.
[23] *Id.* at 311 (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).
[24] *Id.* at 313 (quoting Kyllo v. United States, 533 U.S. 27, 35–36 (2001)).

Carpenter's reasoning maps well to the § 926(a) context. Individual Form 4473 records in a physical filing system or stored as unsearchable PDF images are compliance documents, each one a unique transaction record with little to no analytical significance alone. Those same individual records, aggregated and processed via AI inference, turn into what *Carpenter* calls a "comprehensive dossier", or, in this context, a dossier of firearms ownership that is precisely the kind of knowledge Congress sought to prohibit.[25] The parallel reasoning is not flawless; *Carpenter* is a Fourth Amendment case, and the registry prohibition is statutory. But the aggregation principle applied by the Court, that the collection of individual data points can produce a qualitatively different and constitutionally significant outcome, creates the doctrinal vocabulary for understanding why AI inference on ATF's data holdings raises concerns that the existing registry debate has not properly contended with. Kerr's framework supplies the conceptual architecture; while *Carpenter* demonstrates that the Court has already accepted its core premise in the separate but analogous digital surveillance context.

The doctrinal framework then, is straightforward. The practical question, and the one to which this paper now turns, is what data currently exists within the federal ecosystem that could be used as inputs for inference analysis.

III. Federal and State Data Available for Inferential Analysis

Any examination of whether AI inference poses a reasonable threat to the registry prohibition requires an assessment of the data that is currently held across federal and state systems that could serve as inputs for inferential analysis. While this overview likely only covers a fraction of the true amount of available data, it still reveals a broader data ecosystem than the existing registry debate has acknowledged to date.

The most relevant and concerning data holdings are those ATF directly controls and maintains. The Out-of-Business Records Imaging System (OBRIS) holds those 921 million digitized transaction records from dealers who've closed or surrendered their licenses. The records are images of Form 4473, the form you fill out when you buy a gun from a licensed dealer.[26] Name, address, date of birth, firearm description, serial number. Everything you'd need for a registry, stored as PDFs with optical character recognition (OCR) capability disabled but not deleted.

The disabled OCR safeguard reflects an assumption rooted in legacy software architecture: that preventing text-based search is the same thing as preventing data

[25] *Id.* at 311.
[26] BUREAU OF ALCOHOL, TOBACCO, FIREARMS & EXPLOSIVES, *ATF Form 4473—Firearms Transaction Record Revisions*, https://www.atf.gov/firearms/atf-form-4473-firearms-transaction-record-revisions.

extraction, an assumption modern multimodal AI models do not operate under.[27] Vision transformers and multimodal large language models process document images as visual objects, executing text recognition as an integrated component of visual understanding rather than as a distinct preprocessing step dependent on a separate OCR engine. For models like this, a handwritten serial number on a Form 4473 is a visual entity to be tokenized and structured, not text to be indexed. Removing the search function from a PDF stops a human analyst from performing a document keyword search; it does not offer equivalent resistance to a model trained to extract and structure data from raw image files. Further, the statutory risk does not turn on the inference issue alone. Even without a predictive modeling capability, using tools available today to perform the simultaneous application of text extraction, entity structuring, and record linkage across data in OBRIS could create a database that is searchable and indexed by name, exactly what § 926(a) prohibits.

A balanced assessment of this capability requires acknowledging the difference between technical feasibility and deployment at scale. Processing hundreds of millions of document images through multimodal inference would require massive computational infrastructure, would produce meaningful error rates, and would be a nontrivial resource commitment. The barrier, however, is resource allocation and institutional decision-making, not technical impossibility. Resource barriers are precisely the kind of safeguard that erodes as computational costs decline and model efficiency improves. Therefore, the argument centers on capability as opposed to imminence, and the legal question is whether the statutory framework should account for capabilities whose deployment trajectory is technically possible but not yet in use.

ATF also maintains the Multiple Sales reporting system.[28] When a person purchases two or more handguns from the same dealer within a five-business day window, that dealer is required to report it. That's a dataset specifically designed to flag purchasing patterns.

Then there's eTrace, the web-based system that lets law enforcement trace firearms recovered from crime scenes.[29] It's a query system, not machine learning, but it generates data about where specific guns end up. And the National Integrated Ballistic Information

[27] Geewook Kim et al., *OCR-Free Document Understanding Transformer*, in COMPUTER VISION—ECCV 2022, at 498 (2022), https://arxiv.org/abs/2111.15664 (demonstrating document understanding without reliance on traditional OCR).
[28] BUREAU OF ALCOHOL, TOBACCO, FIREARMS & EXPLOSIVES, *Reporting Multiple Firearms Sales or Other Dispositions* (fact sheet), https://www.atf.gov/firearms/reporting-multiple-firearms-sales-or-other-dispositions.
[29] BUREAU OF ALCOHOL, TOBACCO, FIREARMS & EXPLOSIVES, *eTrace—Internet-Based Firearms Tracing System*, https://etrace.atf.gov.

Network (NIBIN) contains over 7 million ballistic images using correlation algorithms to match shell casings and bullets to specific firearms.[30]

Outside of ATF's own data holdings, other federal agencies collect and maintain data with potential inferential relevance. For example, even though Tiahrt Amendments mandate that NICS background check data is destroyed after a set period (twenty-four hours), metadata patterns, like transaction timestamps, query frequencies, and system interaction logs, could persist independently of the substantive records.[31] Whether such metadata actually persists in accessible form within federal systems is an empirical question this paper cannot definitively resolve. To date, no oversight mechanism, such as a GAO report, OIG audit, or FOIA disclosure, has demonstrated evidence of the retention of disaggregated NICS transaction metadata beyond the mandated period. The danger, however, is not custodial in nature, it's structural. If the system retains any administrative data, like audit logs, system interaction timestamps, or query frequency, that digital residue, even if anonymized, is input for inferential reconstruction when combined with other permanent and wholly retained federal data. Furthermore, this data would not stand alone. The National Firearms Act (NFA) registry tracks data on items subject to NFA regulation, like machine guns, suppressors, and short-barreled rifles.[32] Unlike the out-of-business records, the NFA registry is a lawful, searchable database and its presence and architecture shows that the federal government already maintains a firearms registry for at least one category of firearms. This makes the inferential leap to broader ownership data more tangible. Federal import and export records also document firearms that move across borders, generating yet another data source.

At the state and local government level, visual firearms detection systems represent an emerging parallel data layer of concern. Companies like Evolv Technology and ZeroEyes deploy AI-enabled detection hardware and camera-analysis software across schools, transit systems, and public venues in dozens of states.[33] These systems have major operational limitations. For example, Evolv's New York City subway pilot detected zero firearms across

[30] BUREAU OF ALCOHOL, TOBACCO, FIREARMS & EXPLOSIVES, *National Integrated Ballistic Information Network (NIBIN) Fact Sheet* (June 2025), https://www.atf.gov/media/22631/download.
[31] 28 C.F.R. § 25.9 (2024).
[32] Cohen, *supra* note 3.
[33] Press Release, Evolv Tech., Inc., Evolv Technology Provides Business Update (Jan. 23, 2025), https://www.nasdaq.com/press-release/evolv-technology-provides-business-update-2025-01-23; ZEROEYES, INC., *AI Gun Detection Technology: Enhancing Security and Safety*, https://zeroeyes.com.

twenty stations over the thirty-day pilot period.[34] Separately, a ZeroEyes system at a high school in Tennessee failed to activate during an active shooting because the weapon was never visible to cameras before the shooting started. [35]

The point is not that these systems work well today, and their accuracy is not relevant to the central inference concerns of this paper. The point is that they are proliferating, generating detection and firearms data that did not exist five years ago, and operating alongside parallel identity infrastructure, like ticket scanners, fare card systems, and facial recognition, that could eventually link detections to individuals. Each system has a narrow purpose in isolation. Aggregated computationally with ATF's holdings, NICS metadata, and NIBIN ballistics data, they represent inputs for inferential analysis Congress never contemplated when it wrote the registry prohibition.

IV. The Existing Legal and Legislative Framework

Existing judicial and legislative handling of the registry prohibition issue provides little to no guidance on the question of AI inference. Neither Congress nor the courts have addressed directly whether inferential capabilities applied to ATF's firearms data would violate 18 U.S.C. § 926(a).

The most directly relevant judicial precedent on this issue is *NRA v. Reno*.[36] In that case, the NRA contested the Attorney General's regulations permitting the temporary retention of NICS background check records, arguing the practice violated the registry prohibition. The court disagreed, holding that a six-month retention for purposes of an audit did not create a system of registration because the information was not comprehensive enough.

That comprehensiveness threshold deserves closer examination in view of the current factual circumstances. The *Reno* decision analyzed a six-month window of NICS background check records, a time-bound partial subset of overall firearms transaction data. In *Reno*, the court concluded that the government's limited retention practices were insufficient to be considered a registry. The OBRIS database, by contrast, is the largest and most comprehensive repository of firearms transaction data held on federal servers, and different in kind to the facts at issue in *Reno* as it contains more than 921 million records (spanning

[34] Jake Offenhartz, *Zero Guns Found in New York City Subway in Weapons Scanners Test Powered by Artificial Intelligence*, WASH. TIMES (Oct. 24, 2024), https://www.washingtontimes.com/news/2024/oct/24/zero-guns-found-new-york-city-subway-weapons-scann.
[35] Minyvonne Burke & Jon Schuppe, *AI Weapon Detection System at Antioch High School Failed to Detect Gun in Nashville Shooting*, NBC NEWS (Jan. 23, 2025), https://www.nbcnews.com/news/us-news/ai-weapon-detection-system-antioch-high-school-failed-detect-gun-nashv-rcna189025.
[36] 216 F.3d 122 (D.C. Cir. 2000).

decades and thousands of dealers) retained indefinitely. If comprehensiveness were the operative standard in *Reno*, these records arguably satisfy it, and AI inference would compound the concern by enabling the extraction of structured ownership data from what ATF maintains are unsearchable image files. Yet no court has revisited the question given today's changed factual circumstances, and no court has addressed whether AI inference on legally held data would independently violate the statute.

An important and intervening doctrinal development, however, changes the legal framework for any future challenge. *Reno* was decided under Chevron deference, which gave benefit of the doubt to ATF's interpretation of § 926(a).[37] In June 2024, the Supreme Court overruled Chevron deference in *Loper Bright Enterprises v. Raimondo*.[38] Under Chevron deference, challengers would have had to show that ATF's interpretation was unreasonable. Post-*Loper Bright*, courts decide for themselves what "any system of registration" means. ATF's long-held interpretation would still carry persuasive weight under the *Skidmore v. Swift* framework that survived *Loper Bright*.[39] But persuasive weight is a considerably different posture than the near-dispositive deference *Chevron* afforded, and a court applying independent judgment to the statutory text would have more latitude to evaluate whether "any system of registration" encompasses inferential capabilities that the 1986 Congress could not have foreseen.

The central interpretive question this section raises is what "any system of registration" means under § 926(a) when the mechanism at issue is inferential as opposed to archival. Answering this requires choosing between three competing interpretations. A formal reading, at its narrowest, insists on a structured database organized for lookup by owner name. In essence, a digital equivalent of a filing cabinet. As discussed later in Part VI however, the plain meaning of the term "any system" could support a broader textualist interpretation than this narrow reading allows. A functional reading focuses on the output rather than the architecture, not allowing any mechanism that enables the government to identify gun owners, regardless of how the files are organized. A purposive reading treats the statute as preventing the government from possessing personally identifying firearms ownership knowledge, whether in a database or through computation.[40] The functional reading requires some kind of retrieval mechanism. The purposive reading extends to knowledge the government can derive even without one. This paper contends that the purposive reading

[37] Chevron U.S.A. Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984).
[38] 603 U.S. 369 (2024).
[39] Skidmore v. Swift & Co., 323 U.S. 134, 140 (1944).
[40] For the distinction between textualism and purposivism, see generally John F. Manning, *What Divides Textualists from Purposivists?*, 106 COLUM. L. REV. 70 (2006).

best reflects the statutory text and context. Congress enacted a categorical prohibition, "any system", reflecting a substantive judgment that the federal government should not possess this category of knowledge about its citizens.[41] If AI inference can generate registry-equivalent knowledge without a registry-structured database, the purposive reading recognizes the functional defeat of the statute's objective. The narrowest formal reading, by contrast, would leave the prohibition a dead letter in any technological environment where knowledge can be derived without being stored in traditional database form.

Courts presented with a future challenge would need a workable standard. To that end, this paper proposes a functional equivalence test. The test would ask the following: does the system allow the federal government to achieve any of the three registry-equivalent capabilities articulated in Part II (individual-query, population-enumeration, or reverse-trace), reliably and at scale, irrespective of how the data is stored. This standard preserves the statute's protective intent while offering courts a workable benchmark for modern technology.[42]

Congress has introduced legislation attempting to address different ATF registry issues with little success. For example, in July 2024, Representative Andrew Clyde introduced an amendment to bar funding for ATF's digital registry operations. It passed the House Appropriations Committee 29-25 but did not advance further.[43] The FY2025 Commerce, Justice, Science appropriations bill never received a floor vote. Congress ultimately passed a continuing resolution in place of full-year appropriations, and the Clyde amendment failed without becoming law.

The Full-Year Continuing Appropriations Act, passed in March 2025, simply continued FY2024 funding levels.[44] No new restrictions on ATF, or prohibition on digitization. No requirement to delete all existing records. ATF continues operating OBRIS as it did before.

Other legislative efforts have also emerged. In January 2025, Senator Jim Risch and Representative Michael Cloud introduced the "No REGISTRY Rights Act", which would

[41] S. Rep. No. 98-583, *supra* note 19.
[42] Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding that technology allowing the government to obtain otherwise unobtainable info without physical intrusion constitutes a "search" regardless of the mechanism, functional-equivalence approach to technological circumvention of constitutional limits).
[43] Press Release, H. Comm. on Appropriations, Committee Approves FY25 Commerce, Justice, Science, and Related Agencies Appropriations Act (July 10, 2024), https://appropriations.house.gov/news/press-releases/committee-approves-fy25-commerce-justice-science-and-related-agencies.
[44] Full-Year Continuing Appropriations and Extensions Act, 2025, Pub. L. No. 119-4, 139 Stat. 9 (2025).

require ATF to delete all existing firearm transaction records.[45] The FY2026 appropriations process included similar provisions at the committee level but those provisions were removed during negotiations and the House passed the final bill in January 2026 without them.[46]

Recent litigation over ATF's 2024 "Engaged in the Business" rule offers a window into the current judicial posture toward at least some of the agency's regulatory interpretations.[47] In June 2024, a federal judge granted a preliminary injunction blocking enforcement of the rule in *Texas v. ATF*, holding that it likely overstepped statutory authority.[48] In October 2025, a separate federal court issued a permanent injunction in *Butler v. Bondi*.[49] In January 2026, the Fifth Circuit denied the DOJ's motion to delay or stay proceedings.[50]

While none of these cases involve ATF actions or policies directly related to the registry prohibition issue, they do point to a judiciary seemingly more skeptical of ATF's regulatory interpretations, particularly post-*Loper Bright*.

Gun rights organizations have filed lawsuits challenging ATF record-keeping practices.[51] Privacy rights advocates have raised concerns about AI use in the government.[52] The intersection of these two lines of effort, whether AI inference applied to firearms data violates the registry prohibition, remains unaddressed. Current scholarship is silent on this issue; no law review article, policy paper, or legal brief has addressed this question directly.

V. The Evolution of Federal AI Governance: From Risk Evaluation to Acceleration

The policy environment governing the deployment of AI across the federal government today is the result of two administrations and their markedly divergent approaches. Understanding the current policy trajectory and what it means for firearms data necessitates examining both in more detail.

---

[45] Press Release, Sen. Jim Risch, *supra* note 8.
[46] Chris Eger, *ATF Funding Bill Moving Forward at Near Biden-Era Levels*, GUNS.COM (Jan. 13, 2026), https://www.guns.com/news/2026/01/13/atf-funding-bill-moving-forward-at-near-biden-era-level
[47] Definition of "Engaged in the Business" as a Dealer in Firearms, 89 FED. REG. 29,068 (Apr. 19, 2024), invalidated by Butler v. Bondi, No. 1:24-cv-975-CLM (N.D. Ala. Sept. 30, 2025).
[48] Texas v. Bureau of Alcohol, Tobacco, Firearms & Explosives, No. 2:24-CV-089-Z, 2024 WL 2967340 (N.D. Tex. June 11, 2024).
[49] 805 F.Supp.3d 1175 (N.D. Ala. 2025).
[50] Texas v. Bureau of Alcohol, Tobacco, Firearms & Explosives, No. 24-10612 (5th Cir. Jan. 13, 2026).
[51] Morehouse Enters., LLC v. Bureau of Alcohol, Tobacco, Firearms & Explosives, 78 F.4th 1011 (8th Cir. 2023).
[52] ELEC. PRIVACY INFO. CTR., *Government Use of AI*, https://epic.org/issues/ai/government-use-of-ai/ (last visited Feb. 2026).

The Biden administration's risk mitigation approach to AI governance is anchored in Executive Order 14110, signed in October 2023.[53] The directive created a deliberate and high-friction deployment process, requiring the Department of Justice (DOJ) to catalog AI deployment across areas like sentencing, parole decisions, risk assessments, police surveillance, predictive policing, and forensic analysis. The DOJ did so and delivered a 77-page report in December 2024, cataloging how AI was being deployed across the criminal justice system and recommended safeguards.[54]

OMB in March 2024 released Memorandum M-24-10.[55] It created a category called "rights-impacting AI" that explicitly included law enforcement facial recognition and predictive policing. Government agencies seeking to deploy "rights-impacting AI" were subject to extensive procedural requirements, including independent evaluations, tests for bias, and mandated disclosure to the public. The FBI responded by instituting an AI governance policy in 2024, requiring any new AI capabilities to first get approval through an AI Ethics Council.[56]

A fair assessment of the Biden administration's AI governance framework requires acknowledging both its scope and its limitations. The "rights-impacting AI" category was developed out of concerns about racial bias in predictive policing, discriminatory facial recognition, and algorithmic sentencing disparities. These are well-founded concerns. They are also concerns that emerge from a specific civil liberties tradition that has not historically engaged with the Second Amendment. The Biden administration was not thinking about gun owners when it built its AI guardrails. It was thinking about the communities most likely to be on the wrong end of a predictive policing algorithm or a facial recognition misidentification.

This matters because a reasonable person may see the policy framework and think, at least government policy was asking whether AI in law enforcement raised constitutional

---

[53] Exec. Order No. 14110, 88 Fed. Reg. 75,191 (Nov. 1, 2023), *revoked by* Exec. Order No. 14,148, 90 Fed. Reg. 8,237 (Jan. 28, 2025).

[54] U.S. DEP'T OF JUST., OFF. OF LEGAL POL'Y, *Artificial Intelligence and Criminal Justice: Final Report* (Dec. 3, 2024), https://www.justice.gov/olp/media/1381796/dl.

[55] OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, Memorandum M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (Mar. 28, 2024), https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.

[56] U.S. DEP'T OF JUST., OFF. OF THE INSPECTOR GEN., *Audit of the DEA's and FBI's Efforts to Integrate Artificial Intelligence and Other Emerging Technology Within the U.S. Intelligence Community* (Dec. 19, 2024), https://oig.justice.gov/news/doj-oig-releases-report-deas-and-fbis-efforts-integrate-artificial-intelligence-and-other.

concerns. And that's true, as far as it goes. But the same administration that created "rights-impacting AI" as a category was simultaneously expanding ATF's enforcement posture, finalizing the "Engaged in the Business" rule to broaden who qualifies as a firearms dealer, and overseeing the continued digitization of millions of firearm transaction records every month.[57] The protective framework that animated the Biden administration's policy on AI governance likely did not extend to the intersection of AI and firearms data. There is no indication that any aspect of the administration's policy apparatus was going to ask whether AI inference on ATF's billion records could violate the registry prohibition.

ATF, for its part, has no publicly identified AI-specific policy under any administration. Separately, ATF admitted using Clearview AI facial recognition software, with 549 searches between October 2019 and March 2022.[58] ATF claims to have stopped the practice as of April 2023. Currently, there is no publicly available policy governing what AI capabilities the agency deploys, no disclosure requirements, and no independent evaluation process. This lack of an AI-specific governance at ATF was present during the Biden administration and persists under the current administration today.

Executive Order 14148, signed January 2025, revoked Biden's AI executive order.[59] Three days later, Executive Order 14179 ordered the development of AI that is "free from ideological bias" and required a review of all prior administration actions with regard to AI.[60] The framing around AI moved from a risk evaluation orientation that asked the question "what risks does AI pose?" to an adoption-and-acceleration orientation that asked the question "what barriers are slowing AI adoption?"

OMB's replacement guidance arrived in April 2025 as Memorandum M-25-21.[61] Memorandum M-25-22 followed.[62] These memos didn't merely revise the previous administration's framework; they reoriented it in fundamental ways. For example, Chief AI

[57] Definition of "Engaged in the Business" as a Dealer in Firearms, *supra* note 47.
[58] U.S. GOV'T ACCOUNTABILITY OFF., GAO-23-105607, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training and Policies for Civil Liberties* (Sept. 2023).
[59] Exec. Order No. 14148, 90 Fed. Reg. 8,237 (Jan. 28, 2025).
[60] Exec. Order No. 14179, 90 Fed. Reg. 8,741 (Jan. 31, 2025).
[61] OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, Memorandum M-25-21, *Accelerating Federal Use of AI Through Innovation, Governance, and Public Trust* (Apr. 3, 2025).
[62] OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, Memorandum M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government* (Apr. 3, 2025).

Officers, who previously had been tasked with risk evaluation and ensuring "responsible" deployment, were redefined as "change agents and AI advocates."[63]

The "rights-impacting AI" category disappeared, along with the independent evaluation requirements. Bias testing mandates were replaced with language about avoiding ideological constraints on AI development. By July 2025, Director Kratsios was at CSIS explaining that all government data would be ingested into AI models.[64] By November 2025, the Genesis Mission Executive Order made it official policy within the scientific research domain, establishing institutional precedent and infrastructure for the broader data-ingestion trajectory Kratsios described. [65]

The implications of this policy trajectory for the registry question are significant. The Biden framework, for all its limitations, at least operated from the premise that government AI use in law enforcement contexts warranted special scrutiny. It would likely not have caught the specific problem this article describes, however, as there is no evidence that those who built it were thinking about firearms data. The institutional practice of a robust, if not onerous pre-deployment risk evaluation created the possibility, however remote, that someone in the evaluation chain might have identified the tension between AI inference capabilities and the statutory prohibitions under § 926(a).

Under the current framework, even that remote possibility is largely gone. The federal government's posture on AI has shifted from cautious evaluation to focused acceleration. ATF still has no public-facing AI governance policy. The "rights-impacting" category no longer exists. Chief AI Officers are advocates, not gatekeepers. And the OSTP Director is publicly encouraging the ingestion of all government data into AI models.

Neither administration built a framework that would explicitly protect firearms owners from AI-enabled registry inference. The Biden administration's AI governance apparatus, focused as it was on a different set of civil liberties issues, did not explicitly engage with the problem. The current administration has removed even the general-purpose guardrails that might have incidentally surfaced the issue. The technical capability to infer registry-equivalent information from legally held data either exists or is on the way. The statute

[63] Fact Sheet, OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, *Eliminating Barriers for Federal Artificial Intelligence Use and Procurement* (Apr. 7, 2025), https://www.whitehouse.gov/fact-sheets/2025/04/fact-sheet-eliminating-barriers-for-federal-artificial-intelligence-use-and-procurement/.
[64] Alexandra Kelly, *U.S. Government Will Ingest All Federal Data into AI Models, WH Tech Director Says*, DEF. ONE (July 30, 2025), https://www.defenseone.com/policy/2025/07/white-house-tech-director-breaks-down-plan-balance-ai-national-security-and-export-promotion/407102.
[65] Exec. Order No. 14363 *supra* note 2.

prohibiting a registry remains unchanged, and no one within either administration's AI policy apparatus has or had any institutional reason to address the collision.

VI. Anticipated Objections and Responses

The legal analysis discussed in this paper is likely to elicit several thoughtful objections worth engaging in this section to assist in clarifying key nuances and opposition.

A. *"A registry is not the same thing as inference."*

A registry is a list, a compiled record. Inference is an analytical capability. One cannot obtain an inference through a Freedom of Information Act (FOIA) request. No database field in the current data held states "gun owner: yes/no"

But even through a textualist lens, the objection is not as strong as it seems at first glance. The statute directly states that it prevents "any system of registration of firearms, firearms owners, or firearms transactions or dispositions." To properly answer this objection, let's analyze the relevant terms ("any", "system", and "registration") individually then as a whole ("any system of registration").

First, the term "any" is one of the broadest terms in the English language, defined as "one or some indiscriminately of whatever kind."[66] Congress in 1986 did not specifically prohibit "a database" or a "searchable list," it prohibited "any system," language which, read naturally, covers organized methods and processes, not simply fixed databases or repositories.

Moving to the next term, "system" is defined as "a regularly interacting or interdependent group of items forming a unified whole," and less common but still a valid definition, "a group of devices or artificial objects or an organization forming a network especially for distributing something or serving a common purpose."[67] AI inference components, made up of defined data inputs, computational processing steps, entity extraction, linked records, and structured outputs, is clearly an organized process of regularly interacting group of items forming a united whole. Therefore, it is a system.

Moving on, "registration," as a term describes the "act of recording or enrolling."[68] In this context, this refers to an association between an identified individual and a recorded

[66] United States v. Gonzales, 520 U.S. 1, 5 (1997) (quoting WEBSTER'S DICTIONARY 97 (year)).
[67] *System*, Merriam-Webster, https://www.merriam-webster.com/dictionary/system (last visited Feb. 2026).
[68] *Registration*, BLACK'S LAW DICTIONARY (12th ed. 2024).

attribute, firearms ownership. Examining § 926(a), it does not condition the prohibition on the specific instrument or medium in which the associations are maintained, the format they are stored in, or whether they are generated by hand or computationally. The statute prohibits the system that produces them. AI inference that reliably produces or has the capability to produce person-to-firearm associations performs the functional act of registration each time it undertakes a query, differing from a traditional registry only in that it registers in a dynamic manner versus a static manner. That distinction is at the architecture level, not in the ordinary meaning of the term.

Read as a phrase together, "any system of registration" includes any regularly interacting group of components, regardless of form or medium, that performs the act of recording or enrolling associations between individuals and firearms. A textualist reading of § 926(a), therefore, does not need to contort itself to incorporate AI inference capabilities and pipelines; the statute's plain language allows for it. The Supreme Court has recognized, in related contexts involving the technological circumvention of constitutional rights, that legal rules "must take account of more sophisticated systems that are already in use or in development."[69] Interpreting "system" to refer to only static databases would allow technological circumvention of the prohibition enacted by Congress; a result that is directly opposed to both statutory purpose and the presumption against ineffectiveness that well-executed textualism requires.[70] Additionally, any reading that limits "system of registration" to a specific database architecture would fail the canon against absurd results, rendering the prohibition easily bypassed by any federal agency willing to derive registry-equivalent knowledge via alternative storage and retrieval mechanisms.

A purposive reading is equally compelling independent of the textualist analysis. Congress did not enact § 926(a) because it objected to a particular database architecture. It enacted this law as a deliberate judgment grounded in the belief that the federal government should not collect and maintain comprehensive knowledge of individual firearms ownership, no matter how helpful that may be to law enforcement.[71] The fact that ATF lawfully possesses the underlying records under § 923(g)(4) to conduct tracing fails to address the question. Tracing is a serial number-to-first-purchaser query, a singular, limited inquiry. Registry-equivalent knowledge is something different, the ability to infer associates between an

[69] Kyllo v. United States, 533 U.S. 27, 36 (2001); Carpenter v. United States, 585 U.S. 296, 313 (2018) (citing *Kyllo*).
[70] Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal* Texts 63–65 (2012); Corley v. United States, 556 U.S. 303, 314 (2009) (applying related canon that "a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous").
[71] S. Rep. No. 98-583, *supra* note 19.

individual person and the firearms they own, determine probable owners within a larger group of citizens, or reverse-trace ownership without the authorized process Congress had in mind. The statutory concern was aimed at knowledge, not a specific filing system. If AI inference can produce registry-equivalent knowledge without a registry-structured database, the statutory purpose is effectively defeated, an outcome the textualist analysis above indicates the plain language was broad enough to stop.

Solove's framework strengthens either reading. His argument that "the law should treat data derived from inferences on an equal footing with collected data" supports treating an inferential analysis pipeline as a system that registers ownership within the meaning of § 926(a), irrespective of how the analysis proceeds: from the text or the purpose. Courts have not yet adopted that position, but courts also have not been asked to, particularly in the firearms context.

B. *"This concern is too speculative. ATF isn't actually doing this."*

Today, there's no public evidence that ATF is applying machine learning to its firearm transaction records. eTrace is a traditional database query system. NIBIN uses pattern-matching algorithms that predate modern ML. The agency hasn't disclosed any AI inference capability or any plans to do so, and no such claim is made here.

But the argument advanced in this paper is not primarily about what ATF is doing today. It concerns what becomes technically possible when a billion digitized records are legally held by an agency with no public AI governance usage policy or framework, all while operating under a broad policy directive to ingest all government data into AI models. The policy direction is not unknown or a matter of speculation. The relevant question is whether we address the legal tension before or after the inferential capability is operationalized.

C. *"Courts would never allow this."*

Post-*Loper Bright*, courts are certainly both more willing and more doctrinally empowered to independently scrutinize agency interpretations. Current "Engaged-in-the-Business" litigation demonstrates that judges are not automatically deferring to ATF, so a properly framed challenge to AI-driven inference on firearms data could succeed.

Reliance on judicial review as a safeguard, however, rests on a multitude of dependent assumptions: that a plaintiff with standing brings a properly framed challenge, that the court reaches the merits, and does so before the capability becomes deeply entrenched. Each assumption introduces uncertainty. Moreover, even successful litigation operates on a timeline measured in years, not months. By the time a court rules, the inferential capability

may have already been deployed, the data may already have been processed, and the operative question becomes remediation rather than prevention, a more difficult posture for any challenger. The time problem is further compounded by the speed of technological change: the inferential mechanisms at issue are not static, and the underlying AI capabilities may evolve in complexity or kind during the period of litigation, potentially changing the nature of the constitutional question a court is asked to address. This paper does not undertake the full procedural analysis that any future litigation would require.

D. *"The current administration supports gun rights. It wouldn't do this."*

As a structural safeguard, political alignment and issue support are by nature contingent. Presidential administrations change, and policy positions can shift within a single term. Technical capabilities, once established, persist across administrations. The statute does not condition the registry prohibition on the political views of the current administration. It says no registry.

More to the point, the current administration's own AI policy framework calls for ingesting all government data into models. This is not a speculative projection; this is a stated policy priority. The logic of comprehensive data ingestion does not contain an inherent limiting principle that would exempt particular agencies or categories of records from its application.

E. *"The firearms data in these records is too messy to be considered a usable registry."*

A nontrivial number of the 921 million OBRIS records held by ATF are likely to be images of handwritten forms or of forms that contain some handwritten information. These handwritten records are in some cases likely to be illegible and span across decades of varying documentation practices. Given this, any AI-derived extraction from this material would contain errors or missing context at some error rate, making accurate inference in every case a challenging endeavor. From this, a critic could assert that a "registry" full of errors or inaccuracies is not functionally useful and, therefore, not a "system of registration" as statutorily prohibited.

This critique conflates two different standards: the evidentiary standard for prosecution with the standard for surveillance. A registry does not need to be deterministic to be used as an intelligence tool. An inferential system that produces ownership assessments with meaningful but imperfect confidence can still direct government investigative or surveillance resources in ways Congress sought to prohibit. The statute prohibits "any system of

registration," and it does not condition that prohibition on the system's confidence level or precise accuracy. An error-filled registry is still a registry if it allows the government to, reliably and at scale, infer probable firearms ownership.

F. *"The term 'system' implies institutionally developed architecture. That is not the same thing as simply running an AI model."*

From a skeptical textualist point of view, this is the strongest counterargument. The objection posits that "system of registration" means something intentionally built, maintained, and always available. So, a registry structure, not a singular analytical query. From this point of view, running inference queries in OBRIS is akin to performing analysis, not constructing a registration, in the same way that a researcher combing through paper Form 4473 records is performing research, not registry-building. The "system" in this argument is the filing cabinet, not the person reading through it.

This objection fails in two ways. First, the difference between what we call "analysis" and "system" falls apart when the capability (AI inference) is repeatable, scalable, and available on demand. A single, limited, ad hoc query by a researcher could be considered analysis. An inferential analysis pipeline, by contrast, that is built, validated, operational, and available for repeated use by authorized persons is a "system" by the ordinary understanding of the word.[72] It would contain clear inputs (such as images in OBRIS, eTrace records, Multiple Sales data), defined processing steps (entity extraction, record linkage, probabilistic matching), and defined outputs (person-to-firearm ownership associations). It can be done repeatedly and can produce consistent results. That is a "system" defined in the ordinary way, "a regularly interacting or interdependent group of items forming a unified whole," or "a group of devices or artificial objects or an organization forming a network especially for distributing something or serving a common purpose."[73] The question is not whether an analyst could determine ownership information from scattered records manually; a determined analyst always could. The question is whether the government has created or could create an organized, repeatable process for doing so. An inferential analysis pipeline is exactly that.

Second, the objection assumes that § 926(a) necessitates the intentional establishment of a registry as a conscious institutionally driven act. But the statute does not say "no agency

[72] AI systems deployed federally need authorization to operate (ATO) and may be subject to high-impact designation under OMB M-25-21 § 3. Any model that passes ATO and agency review would be a system both technically and administratively. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073.
[73] *System*, *supra* note 67.

shall establish" a system of registration. It says the Attorney General shall not "prescribe rules or regulations" that "require" a system of registration, and, at a broader level, that no such system shall exist "under the provisions of this chapter."[74] The prohibition relates directly to the existence of the system, not to the subjective intent driving its creation. An inferential analysis pipeline that produces registry-equivalent knowledge violates § 926(a) regardless of anyone's intent to set out and build a "registry."

VII. The Chilling Effect of Inferred Government Knowledge

The implications of AI inference on firearms data go beyond § 926(a) and raise constitutional concerns grounded in the chilling-effect doctrine.

The Supreme Court has long acknowledged that government surveillance can chill the exercise of constitutional rights even when no follow-on enforcement action occurs. In *Lamont v. Postmaster General* (1965) the Court invalidated a requirement that individuals who receive "communist political propaganda" must affirmatively request delivery from the Post Office.[75] The constitutional inadequacy recognized by the Court was not that individuals were being punished for reading communist literature, but that the government maintained a mechanism for monitoring those who requested it via the post office. The surveillance function alone, independent of any enforcement, was sufficient to chill First Amendment activity.

NAACP v. Alabama (1958) reflects the same legal principle: the Court held that compelled disclosure of membership lists would chill freedom of association under the First Amendment. [76] Alabama did not claim any intent to prosecute NAACP group members; the state's stated rationale was that it merely wanted to know who they were. The Court concluded that the burden on associational freedoms arose from the disclosure of the list itself, not any follow-on enforcement action. The principle these cases demonstrate is that government collection of knowledge about the exercise of fundamental constitutional rights can, standing alone, impose an unconstitutional burden.

Applied to firearms data, the relevant question is whether that perception, regardless of its truth or follow on actions, would deter citizens from exercising their Second Amendment rights.[77] The chilling-effect framework as laid out in *Lamont* and *NAACP v. Alabama* (1958)

[74] 18 U.S.C. § 926(a).
[75] Lamont v. Postmaster Gen., 381 U.S. 301 (1965).
[76] NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958).
[77] District of Columbia v. Heller, 554 U.S. 570 (2008); N.Y. State Rifle & Pistol Ass'n, Inc. v. Bruen, 597 U.S. 1 (2022).

support this view as a matter of principle, with the caveat that extending First Amendment doctrine into the Second Amendment context faces unique hurdles. To date, no courts have extended the chilling-effect doctrine to Second Amendment claims. The argument that follows contends that the doctrinal gap has narrowed to the point where extension is now viable.

Courts developed the chilling-effect framework in a specific historical context that included the McCarthy era and civil rights suppression, where the connection between government knowledge and subsequent persecution was demonstrated, not hypothetical.[78] The Second Amendment's regulatory tradition is different. Firearms transactions already require background checks as a statutory precondition of purchase; a form of government awareness the Second Amendment has been held to tolerate. A critic would argue that firearms owners already accept a degree of government knowledge that readers of communist literature in *Lamont* did not.

A deeper objection relates to causal mechanisms. In *Lamont*, recipients knew their mail was being watched because the statute required an affirmative request for delivery. Likewise, in *NAACP*, group members were aware that the state had demanded their names. In both, known surveillance was the causal mechanism for the "chill." AI inference on backend firearms data occurs without notifying the people whose ownership it infers. The objection, thus, runs as follows: if firearms owners do not know the capability exists or that it is occurring, they cannot be "chilled" by it. This objection highlights a real gap in this analogy but draws the wrong conclusion from it. Two theories of harm address the causal challenge at issue here.

The first relates to disclosure. New government capabilities rarely remain unknown to the public forever. The application of an AI inference capability to firearms data would be subject to discovery through various methods, including FOIA requests, congressional oversight, inspector general audits, whistleblower disclosures, or journalistic investigation. Once the information is known to the public, the chilling effect sets in quickly and is easy to recognize.[79] Firearms owners who discover that ATF (or other agencies) can computationally infer ownership profile information from transaction records and other correlated data would

[78] The doctrine's first expression appeared in Justice Frankfurter's concurrence in Wieman v. Updegraff, 344 U.S. 183, 195 (1952) (Frankfurter, J., concurring), involving loyalty oaths forced on state employees during the Red Scare. It reached its clearest articulation in cases involving civil rights organizations, in NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 462–63 (1958); and Dombrowski v. Pfister, 380 U.S. 479, 487 (1965).

[79] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013) (acknowledging that surveillance programs, once public, may lead to cognizable injury).

face the exact same deterrent as *Lamont's* mail recipients and *NAACP*'s members. There is no requirement in the doctrine that a surveillance mechanism be known when it's created; it does require, however, that once the mechanism is known that it deters the exercise of constitutional rights.

The second theory is structural and independent of public awareness. Section 926(a) is the result of a congressional intent to prevent the federal government from possessing comprehensive firearms ownership knowledge, not merely that it should refrain from publishing that knowledge. As repeatedly stated, the statute prohibits the existence of the system itself, not its disclosure to the public. A government that can reliably identify probable firearms owners is in possession of a tool ready to be used for enforcement, targeting, or political purposes whenever it desires, under any administration.

Congress knew this fact when it enacted § 926(a). The statute was not the result of a documented misuse of registry data, but by the judgment that the existence of the capability or the potential capability was a dangerous enough prospect to proactively prohibit.

Beyond the causal mechanism, two doctrinal developments have fundamentally shifted the legal ground. First, *District of Columbia v. Heller* (2008) and *N.Y. State Rifle & Pistol Ass'n, Inc. v. Bruen* (2022) elevated Second Amendment rights to individual-right status with a historical-tradition analysis that parallels the solicitude the Court has shown First Amendment freedoms. [80] If the right is of comparable constitutional stature, the doctrinal protections attending government surveillance of its exercise should follow. Second, there is a qualitative difference between a temporally limited background check, designed to verify eligibility at the point of sale, and a persistent, computationally derived ownership profile. The former is a gatekeeping function; the latter is surveillance. The chilling-effect doctrine ultimately turns on a single, operative question: does the mere fact of government knowledge discourage the exercise of constitutional rights?

The answer to that question is not self-evident. Within the disclosure-based theory, how individuals will react to perceived government surveillance will differ, but, at the margins,

[80] District of Columbia v. Heller, 554 U.S. 570, 592, 595 (2008) (holding the Second Amendment protects "an individual right to keep and bear arms" and often analogizing to First Amendment protections); N.Y. State Rifle & Pistol Ass'n v. Bruen, 597 U.S. 1, 24 (2022) ("This Second Amendment standard accords with how we protect other constitutional rights. Take, for instance, the freedom of speech in the First Amendment, to which Heller repeatedly compared the right to keep and bear arms."). For an analysis from scholars of the *Bruen*'s assertion that its historical-tradition methodology parallels First Amendment analysis, see Clay Calvert & Mary-Rose Papandrea, *The End of Balancing? Text, History & Tradition in First Amendment Speech Cases After* Bruen, 18 DUKE J. CONST. L. & PUB. POL'Y 59, 60–66 (2023).

perception affects behavior, and it is at the margins that this doctrine lives. Under the structural theory, the injury does not rely on any one person's subjective response; it lies in the government's ability to perform the capability itself, which Congress determined was incompatible with an armed citizenry's rights.

A database of firearm transaction images, searchable only by serial number through a manual query process, presents one set of constitutional concerns. That same database, processed through AI inference to generate individual ownership probability assessments or other data, presents a materially different concern. The formal data structure may be identical in both scenarios, but the practical effect on the constitutional interests § 926(a) was enacted to protect is fundamentally changed. Whether the courts will adopt a framework that validates this distinction is a question that remains to be answered. The central technical reality at issue in this paper, however, is difficult to deny: AI inference as an emerging capability fundamentally modifies the legal character and constitutional status of lawfully possessed government data, firearms or otherwise. The statute, § 926(a), as currently drafted, does not distinguish between these realities. This paper contends that it should, and that courts, presented with the question, have adequate doctrinal foundation in the chilling-effect case law to reach that conclusion.

Conclusion

This paper opened with a discrete factual predicate: the OSTP Director's public description of a policy vision in which all government data is fed into AI models.

Director Kratsios described a vision in which all categories of government data, tax records, healthcare data, permitting systems, would be incorporated into AI models to deliver citizen services. The remarks were directed at an international audience and framed as an argument for the superiority of the American technology stack.

His remarks were not directed at firearms' data. ATF, however, is a federal agency, and its 921 million digitized firearm transaction records are government data. The records are currently maintained on federal servers and as the former ATF Director admitted, one of the primary barriers between these files and a searchable registry is a disabled software feature.

Congress confronted the prospect of a federal firearms registry four decades ago and enacted an unqualified prohibition. The Firearm Owners' Protection Act did not condition the prohibition on considerations of administrative utility or technological feasibility. It reflected an absolute principle: certain categories of federal government knowledge about a citizen's exercise of constitutional rights are too dangerous to allow regardless of any efficiencies or administrative value they may possess.

That principle is now in direct tension with an administrative policy that seeks to treat all government data as appropriate material for AI model training and is prioritizing efficiency through AI adoption. The statutory prohibition, despite legislative attempts, has not been amended. Technology has leapfrogged the legislative safeguards of the 1986 law. The friction of manual record-keeping, which Congress once relied upon to prevent constitutional violations, no longer limits what the government can learn from lawfully held data. With an administration turning toward rapid AI deployment, the institutional checks or policies that could have flagged violations of this statute are largely gone, in favor of speed and efficiency.

As a result, there are really only two publicly known barriers to an AI-inferred shadow national firearms registry. One is the current administration's generally favorable disposition toward Second Amendment issues, which we have already stated could change like any other policy. The second is essentially a contractual vendor setting: ATF pays Adobe to disable search functionality in files containing the personal firearms transaction data of millions of Americans. In an era of commodity OCR, entity extraction, record linkage, and inference, a software toggle is a fragile mechanism for maintaining a statutory prohibition.

Several policy responses are available. Congress could amend § 926(a) to reach functional equivalents and inferential reconstruction. This can be done, for example, by redefining "system of registration" to include any computational process that allows the government to derive firearm ownership determinations from federal data, regardless of how the data files are stored. Alternatively, Congress or the Executive branch could categorically exclude firearms transaction records from all data ingestion initiatives and mandate that ATF create a public-facing AI governance policy. A narrower response would exempt records subject to statutory access restrictions from federal AI data-sharing and model-training programs. On the litigation side, plaintiffs pursuing challenges would also have viable avenues outside of § 926(a) itself. The Privacy Act of 1974 independently limits what federal agencies can do with personally identifiable information (PII). The Act defines a "system of records" as:

> a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.[81]

AI inference processes that analyze OBRIS images, eTrace data, or other data holdings to produce indexed individual identifier outputs (that is, any system achieving the individual-query capability described in Part II), would arguably create a "system of records" and bind it to the Act's notice, consent, and disclosure requirements, none of which ATF has currently

[81] 5 U.S.C. § 552a(a)(5); *id.* § 552a(a)(4) (defining "record").

satisfied or could satisfy without additional rulemaking.[82] The Privacy Act therefore provides a separate statutory basis and avenue for challenging AI-driven transformation of firearms data, one independent of § 926(a)'s interpretive questions. The recent flurry of litigation challenging the DOGE initiative's ability to access federal databases at various federal agencies demonstrates that courts are actively enforcing the Privacy Act's limits on access to federal records containing PII, even when the government asserts legitimate purposes for that access.[83]

In 1986, Congress intended to prohibit a federal firearms registry and legislated to do so. It did not, and in 1986, could not, have been expected to prohibit the inferential reconstruction of registry-equivalent knowledge from lawfully held data. That gap now requires an answer.

[82] 5 U.S.C. § 552a(e)(4); *id.* § 552a(b) (requiring agencies to publish notice before keeping a system of records; and disclosure without a written consent is disallowed without an exception).
[83] Peter J. Benson & Chris D. Linebaugh, CONG. RSCH. SERV., LSB11370, *Privacy Act Lawsuits and the Department of Government Efficiency (DOGE)* (Sept. 2025) (list of active challenges as of the date of the report).