BENBROOK LAW GROUP, PC
BRADLEY A. BENBROOK (SBN 177786)
STEPHEN M. DUVERNAY (SBN 250957)
701 University Avenue, Suite 106
Sacramento, CA 95825
Telephone: (916) 447-4900
Facsimile: (916) 447-4904
brad@benbrooklawgroup.com
steve@benbrooklawgroup.com

Attorneys for Plaintiffs

SUPERIOR COURT OF CALIFORNIA

COUNTY OF SAN DIEGO

ASHLEYMARIE BARBA; FIREARMS POLICY COALITION, INC.; SECOND AMENDMENT FOUNDATION; CALIFORNIA GUN RIGHTS FOUNDATION; SAN DIEGO COUNTY GUN OWNERS PAC; ORANGE COUNTY GUN OWNERS PAC; and INLAND EMPIRE GUN OWNERS PAC,

Plaintiffs,

v.

ROB BONTA, in his official capacity as Attorney General of California,

Defendant.

Case No.: 37-2022-00003676-CU-CR-CTL

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT

Hearing: April 18, 2025
Time: 1:30 p.m.
Judge: Hon. Katherine A. Bacal
Department: C-69

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Constitutional Provisions

I. INTRODUCTION

This case arises out of the Legislature's unprecedented requirement that the private information of millions of California firearm owners be disclosed for "research." After 25 years of telling Californians that the personal identifying information (PII) they had to disclose in order to buy a firearm would only be provided by the Department of Justice (DOJ) to other government officials for law enforcement purposes, the Legislature went back on those legislative assurances. At the urging of private researchers at UC Davis, the Legislature enacted AB 173 to now *require* that all of gun purchasers' private information *must* be disclosed to social scientists at UC Davis (and may be shared with countless other researchers) for a very different reason than the PII was collected: to conduct research into violence perpetuated with firearms by using their confidential data to "follow" California gun owners for years. The victims of this disclosure weren't even informed, let alone offered an opportunity to consent.

Plaintiffs are entitled to summary judgment on their claim that AB 173's mandatory data-sharing provisions violate plaintiffs' right to privacy under Article 1, § 1 of the California Constitution. The threshold elements for a constitutional privacy claim, set forth by the California Supreme Court in *Hill v. Nat'l Collegiate Athletic Ass'n* (1994) 7 Cal.4th 1, designed to weed out "de minimis" claims, are readily satisfied by the egregious bait and switch here:

First, Plaintiffs have a legally protected privacy interest in the detailed personal information (including home address, fingerprints, and driver's license numbers) collected by DOJ during firearm and ammunition transactions; this point is not disputed.

Second, individuals purchasing firearms and ammunition have an objectively reasonable expectation that the confidential information they had to turn over to DOJ would not be used for purposes unrelated to law enforcement, much less be disclosed to a private third party, hostile to their interests, for "research" on them. Among other things, Penal Code section 11106 assured them for 25 years that this confidential data could only be transferred within the government for law enforcement purposes.

Third, the disclosure is a serious invasion of privacy—the test requires only that it be "nontrivial"—as AB 173 deprives millions of Californians of control over their personal

information, which will be actively used, mined, and manipulated without their knowledge or consent.

Because Plaintiffs have satisfied this threshold inquiry, this Court turns to *Hill*'s general balancing test.[1] The Court of Appeal has held that the State has a legitimate countervailing interest in promoting firearms research to inform policymaking, so, under the appellate court's interpretation of the cases, Plaintiffs must identify "feasible" and "effective" alternative courses of conduct that "have a lesser impact on privacy interests." *Hill*, 7 Cal.4th at 40. They have done so. DOJ can provide notice to those in the State's databases—and to future firearm and ammunition purchasers—that their PII may be shared with researchers and give them the opportunity to opt out of (or opt in to) such sharing. DOJ could also anonymize or de-identify information from the database. And so far as Plaintiffs are concerned, each of these alternatives are "effective," in that either alternative would in fact "have a lesser impact" on their privacy interests. *Id.* at 40. The parties have agreed that this issue will be subject to further discovery after DOJ files its cross-motion for summary judgment with supporting declarations from its principal witnesses. Plaintiffs will therefore address the issue of "feasible" and "effective" alternative courses of conduct in further detail in their consolidated reply and opposition brief.

Plaintiffs have established a violation of the constitutional right to privacy. Summary judgment should be entered in their favor.

II. BACKGROUND

A. California Law Requires Purchasers Of Firearms And Ammunition To Disclose Extensive Personal Information To DOJ.

To buy a firearm or ammunition in California a purchaser must provide extensive personal identifying information to the vendor, who in turn provides that information to DOJ at the time of the transaction. Various provisions of California law require DOJ to collect a wide array of data related to firearms ownership, and to maintain such information to assist in criminal and civil

[1] The Court of Appeal expressly declined to consider whether Plaintiffs satisfied *Hill*'s threshold factors and decided the preliminary injunction appeal on the balancing test alone. Because this case will likely be the subject of a further appeal, the Court should address each of *Hill*'s factors in resolving the parties' competing motions for summary judgment.

investigations. Principal among the DOJ's databases is California's Automated Firearms System ("AFS"), an omnibus repository of firearm records established by Penal Code section 11106. AFS is the state's most comprehensive database of information about the purchase, sale, transfer, and use of firearms and ammunition.

The database includes the following identifying information (and more) for California gun owners:

- Fingerprints
- Driver's license or identification card number
- Home address
- Date and place of birth
- Citizenship status and immigration information
- Race
- Sex
- Height, weight, hair color, and eye color

See Penal Code § 11106(a)(1)(A) (fingerprints) & (D) (Dealers' Records of Sale of firearms); 11 CCR § 4283 (information required for basic ammunition eligibility check); *see generally* Ex. 2, Cal. Dep't of Justice Bureau of Firearms, *Dealer's Record of Sale (DROS) Worksheet*, https://des.doj.ca.gov/forms/DROS_Worksheet_BOF-929.pdf. AFS also includes all firearm and ammunition transactions associated with each individual. *See* Penal Code § 28160 (content of register of firearm transfers). And for private-party sales or transfers, AFS includes all of this information for the seller as well. *See* Penal Code § 28160(a)(36).

In addition to compiling all information obtained in connection with every firearm and ammunition transaction conducted through a dealer, AFS collects records related to the possession or use of firearms, including: copies of licenses to carry firearms and carry applications; firearm records transmitted to the DOJ outside of the electronic DROS process; reports of stolen, lost, or found property; records relating to the ownership of manufactured or assembled firearms; and a registry of private-party firearm loans. Penal Code § 11106(a)(1)(B), (C), (E)–(G), (I), (b)(2).

Californians have been required to disclose this personal information to the government in order to purchase a handgun since 1996.[2] The Legislature expanded AFS to include long guns beginning January 1, 2014. *See* Assem. Bill 809 (2011-2012 Reg. Sess.). Over the past 25 years, AFS has amassed information covering over 7 million handgun transactions and over 3 million long gun transactions from Dealer Record of Sale ("DROS") data alone. Cal. Dep't of Justice, *Gun Sales in California, 1996–2020*, https://openjustice.doj.ca.gov/data-stories/gunsales-2020.

B. Until AB 173, California Law Assured Gun Owners That Their Private Information Would Remain Confidential And Could Only Be Used Strictly For Law Enforcement Purposes.

From the creation of AFS in 1996 until September 2021, California law treated AFS records as confidential and restricted DOJ's disclosure of PII in the database except when it was necessary to share such information with other government officers for law enforcement purposes. Indeed, since the statute's enactment, the Penal Code has expressly stated that the purpose of DOJ's collection of data in AFS is "to assist in the investigation of crime, the prosecution of civil actions by city attorneys . . ., the arrest and prosecution of criminals, and the recovery of lost, stolen, or found property." Penal Code § 11106(a)(1).

Consistent with this purpose, Section 11106 had always imposed strict conditions on sharing information from the database. Specifically, it provides that the Attorney General "shall furnish the information" in AFS "upon proper application" to specified state officers for criminal or civil law enforcement purposes, including peace officers, district attorneys and prosecutors, city attorneys pursuing civil law enforcement actions, probation and parole officers, public defenders, correctional officers, and welfare officers. Penal Code § 11106(a)(2); *see* Penal Code § 11105. Despite several intervening amendments to Section 11106, this limitation on sharing PII remained consistent from 1996 until the passage of AB 173.[3]

---

[2] As enacted, Section 11106 had initially limited DOJ's retention of AFS records to "pistols, revolvers, or other firearms capable of being concealed upon the person." Penal Code § 11106(a), (b)(1), (b)(2), (c)(1) (West 1997).

[3] *See* Penal Code § 11106(a) (West 1997) ("In order to assist in the investigation of crime, the arrest and prosecution of criminals, and the recovery of lost, stolen, or found property, the Attorney General shall keep and properly file" AFS records, "and shall, upon proper application therefor, furnish to the officers mentioned in Section 11105[.]").

DOJ's privacy disclosures have likewise assured Californians that when they submit their PII to DOJ, it will be treated confidentially and generally used for law enforcement purposes or otherwise only shared with government agencies.

> **Possible Disclosure of Personal Information:** In order to process a request for firearm records, we may need to share the information you provide us with any Bureau of Firearms representative or any other person designated by the Attorney General upon request. The information you provide may also be disclosed in the following circumstances:
>
> - With other persons or agencies when necessary to perform their legal duties, and their use of your information is compatible and complies with state law, such as for investigations, licensing, certification, or regulatory purposes;
>
> - To another government agency as required by state or federal law.

Exs. 3 & 4, Cal. Dep't of Justice Bureau of Firearms, *Automated Firearms System (AFS) Request for Firearm Records* (BOF 053), p. 2; Exs. 5 & 6, Cal. Dep't of Justice Bureau of Firearms, *Personal Firearm Eligibility Check Application* (BOF 116), p. 4. Nothing in these notices informs individuals that their personal identifying information could be shared outside of the government for research purposes. DOJ's Privacy Policy likewise strengthens the expectation of privacy in personal information provided to the agency. It explains:

> **We strive in each instance to tell people who provide personal information to the Department the purpose for which the information is collected.** At the time of collection, we also strive to tell persons who are asked to provide personal information about the general uses that we will make of that information.

Cal. Dep't of Justice, *Privacy Policy Statement*, https://oag.ca.gov/privacy-policy. Despite assuring citizens that DOJ will tell them about the purposes for which the agency will use the personal information it collects, DOJ has never disclosed that one of the known purposes is research.

The expectation of privacy in firearm-related records was reaffirmed by the voters' enactment of Proposition 63 in 2016, which established a background-check requirement for ammunition transactions. Ammunition vendors must collect personal information from each purchaser or transferee and transfer that information to DOJ for collection in the "Ammunition Purchase Records File." Penal Code § 30352(a), (b). Similar to Section 11106, Proposition 63 placed strict limits on the use and disclosure of personal information in the course of ammunition transactions: As enacted by the voters, information collected by DOJ "shall remain confidential and

may be used by [DOJ and other law enforcement agencies in Penal Code § 11105] only for law enforcement purposes." Penal Code § 30352(b).

C. AB 173 Upended This Regime By Requiring DOJ To Disclose The PII Of Millions Of California Gun Owners To Non-Law-Enforcement "Researchers" Without Their Knowledge Or Consent.

The California Legislature drastically altered the landscape when it passed Assembly Bill 173 in 2021. AB 173 requires DOJ to share firearm-related information with the recently-established California Firearm Violence Research Center at UC Davis ("the Center"), and it permits DOJ to share the same information with an unlimited number of other research institutions.[4] AB 173's private-information-disclosure provisions are codified at Penal Code sections 11106(d) and 30352(b)(2).

AB 173 marked a sweeping change to the previous privacy regime. Among other provisions, AB 173 amended Penal Code section 11106(d) to require DOJ to give the Center access to "all information" in AFS "for academic and policy research purposes upon proper request and following approval by the center's governing institutional review board when required." And the bill similarly authorizes DOJ to share this information with "*any other* nonprofit bona fide research institution accredited by the United States Department of Education or the Council for Higher Education Accreditation for the study of the prevention of violence." Penal Code §§ 11106(d) & 14240(a) (emphasis added); *see also* Penal Code § 30352(b)(2) (providing same information-sharing arrangement for personal information in the Ammunition Purchase Records File). The millions of new research subjects were not provided notice of this change, much less an opportunity to opt out of being "followed" by private researchers. Moreover, despite adopting the private researchers' arguments about the importance of this research, AB 173 does not call for the State to pay for it. Rather, the research is often funded by private foundations who vigorously oppose the exercise of firearms rights.

[4] The Legislature established the Center in 2016. Assem. Bill 1602 (2015-2016 Reg. Sess.). The Center's three research mandates are studying (1) "[t]he nature of firearm violence, including individual and societal determinants of risk for involvement in firearm violence . . ."; (2) "[t]he individual, community, and societal consequences of firearm violence"; and (3) "[p]revention and treatment of firearm violence at the individual, community, and societal levels." Penal Code § 14231(a)(1)(A)–(C).

In fact, AB 173 was spurred by a dispute between the Center and DOJ over DOJ's refusal to share the very same PII at issue in this case *based on DOJ's concerns that sharing this data violated gun owners' privacy rights*. *See, e.g.*, Ex. 7, Wiley, *Gun violence researchers fight California Department of Justice's plan to withhold data*, Sacramento Bee (March 15, 2021);[5] Ex. 8, Beckett, TheGuardian.com, *California attorney general cuts off researchers' access to gun violence data* (March 11, 2021). In the past, DOJ had provided the Center with confidential gun owner PII in violation of California law: Multiple research papers affirm that the Center obtained and used gun owner PII in violation of Section 11106. *See, e.g.*, Ex, 9, Zhang et al., *Assembly of the LongSHOT cohort: public linkage on a grand scale*, 26 Injury Prevention 153 (2020) (cross-referencing DROS database, voter registration data, and mortality data to link individual-level data of millions of Californians based on their PII); Ex. 10, Pear et al., *Criminal charge history, handgun purchasing, and demographic characteristics of legal handgun purchasers in California*, 8 Injury Epidemiology 7 (2021) (cross-referencing AFS and DROS databases with criminal charge and conviction history based on PII and evaluating individual demographic characteristics including age, race, and sex); *see also* Ex. 15, Wintemute Prelim. Inj. Decl., ¶¶ 9–14.

In 2020 and 2021, however, DOJ advised the Center that it was going to start complying with the law and no longer provide gun owners' PII for the Center's research. Wiley, *supra* (DOJ spokesman stating "[w]e . . . take seriously our duty to protect Californians' sensitive personally identifying information, and must follow the letter of the law regarding disclosures of the personal information in the data we collect and maintain"); Beckett, *supra* ("it's precisely this more detailed personal information . . . that [then-Attorney General] Becerra's justice department is telling some researchers that it will not provide"; DOJ "cited privacy concerns as a justification for the data restrictions, and has said it believes current California law does not permit the agency to release certain kinds of data to researchers"); *see also* Ex. 13, June 30, 2020 Letter from Randie Chance to Garen Wintemute (AG0000013–14); Ex. 14, Aug. 3, 2020 E-mail from Ashley Ayres (AG0000006–12). DOJ acknowledged earlier in this litigation that "the former Attorney General refused to provide

[5] Dr. Wintemute vouched for the assertions in this article in his declaration opposing Plaintiffs' preliminary injunction motion. Ex. 15, Wintemute Prelim. Inj. Decl. ¶¶ 12–13.

researchers with certain data in the Department's possession." Defendant's Prelim. Inj. Opp. at 11:3–4; *see also* Ex. 15, Wintemute Prelim. Inj. Decl., ¶¶ 11–13. DOJ also instructed the Center to *delete* the PII it possessed from prior disclosures. Beckett, *supra*.

Dr. Wintemute lashed out against DOJ's change in position, and he dismissed DOJ's view at the time that disclosing gun owners' PII raised serious privacy issues: "People have started to wonder what other reasons there might be for which privacy is a fig leaf." Beckett, *supra* (quoting Dr. Wintemute). Wintemute even took the remarkable position that gun owners' PII is "public information" since it was held by DOJ. Orr, *AG Becerra Takes Heat for DOJ's Move to Restrict Release of Gun Violence Data*, KQED (March 12, 2021). He rallied the Legislature to change the law. Ex. 15, Wintemute Prelim. Inj. Decl., ¶ 14.[6]

D. Procedural History.

Plaintiffs filed this lawsuit challenging the constitutionality of AB 173 in January 2022 and filed the operative complaint in June 2022. Plaintiff Ashleymarie Barba is a San Diego County resident who has completed multiple firearm and ammunition transactions (purchase, loan, sale, or transfer) through a firearms dealer in California since 2020. Barba Decl., ¶¶ 2–3. Accordingly, Barba's PII is contained in AFS and the Ammunition Purchase Records File. Barba Decl., ¶ 3. And DOJ has confirmed that Plaintiffs' personal identifying information has been shared with the California Firearm Violence Research Center and other researchers pursuant to AB 173. Ex. 16, Simmons Prelim. Inj. Decl., ¶¶ 17–18, 20.

Plaintiffs Firearms Policy Coalition, Inc.; Second Amendment Foundation; California Gun Rights Foundation; San Diego County Gun Owners PAC; Orange County Gun Owners PAC; and Inland Empire Gun Owners PAC are organizations with members who live in California and who have PII in AFS and the Ammunition Purchase Records File. Combs Decl., ¶¶ 3–4; Gottlieb Decl., ¶ 3; Hoffman Decl., ¶ 3; Schwartz Decl., ¶¶ 2–5 *see also* Barba Decl., ¶¶ 3–4, Schwartz Decl., ¶¶ 8–

[6] The Center took the position that it should have been provided PII under Penal Code § 14231(c)'s language directing DOJ to "provide to the center, upon proper request, the data necessary for the center to conduct its research," ignoring that such sharing was still "[s]ubject to the conditions and requirements established elsewhere in statute," including Penal Code section 11106.

10 (confirming that they have been personally subject to AB 173's information-sharing and object to such disclosure).

Plaintiffs filed a motion for a preliminary injunction in March 2022 based on their claim that AB 173's mandatory data-sharing provisions violate plaintiffs' right to privacy under Article 1, § 1 of the California Constitution.[7] In November 2022, this Court granted the motion and preliminarily enjoined DOJ from engaging in future sharing of PII under AB 173.

A year later, in November 2023, the Court of Appeal reversed.[8] The appellate court first held that this Court did not apply the correct legal standard when ruling on the preliminary injunction. Slip Op. at 21–25. Specifically, the Court of Appeal reasoned that the preliminary injunction ruling committed error by "over[looking] the second step of the two-part inquiry set forth in *Hill*," and therefore "did not apply the full, or correct, legal standard" in ruling that Plaintiffs had established a likelihood of success. *Id.* at 24.

The Court of Appeal next held that Plaintiffs had failed to establish a likelihood of success on the merits. Slip Op. at 25–41. In doing so, the court expressly did not rule on *Hill*'s three threshold elements and instead proceeded to its interest-balancing inquiry. *Id.* at 25–26. On that portion of the analysis, the appellate court then held that the State had established that AB 173's privacy intrusion substantively furthered a countervailing interest in conducting "empirical research supporting informed policymaking aimed at reducing and preventing firearm violence." *Id.* at 26–34.

Finally, the Court of Appeal turned to whether Plaintiffs had adequately showed under the *Hill* test that "there are feasible and effective alternatives to [DOJ's] conduct which have a lesser impact on privacy interests." *Hill*, 7 Cal.4th at 40; *see* Slip Op. at 34–41. On that score, Plaintiffs argued that the State had two specific alternatives to minimize the intrusion on privacy interests: (1) individuals should be given notice of each data request and provided an opportunity to opt out of (or opt in to) having their information shared with researchers; and (2) DOJ could restrict sharing of PII by implementing protective procedures that anonymize or de-identify data shared with researchers.

[7] The FAC included two additional claims that have since been dismissed.

[8] A copy of the Fourth District's opinion is attached as Ex. 17 to the evidentiary compendium.

The Court of Appeal held that neither of these proposed alternatives were feasible and effective based on the evidentiary record at the preliminary injunction stage. Slip Op. at 34–41. As to the notice and opt-out alternative, the court accepted DOJ's argument that "it was not feasible because it would create selection bias that would undermine the results of the studies." *Id.* at 36. The court reviewed the declarations submitted by the State's witnesses to support the general conclusion that an opt-out mechanism would not be "feasible" because it would compromise the State's ability to achieve its research goals. *Id.* at 36–39.

As for the second alternative (anonymizing or de-identifying PII), the Court of Appeal accepted DOJ's assertions that it was already taking equivalent measures for research projects where it was appropriate to do so. Slip Op. at 39 (quoting researcher's declaration stating that "deidentifying data before sharing it with researchers is entirely appropriate," and "[a] core principle in the responsible conduct of research involving sensitive data is the 'minimum necessary' principle"); *id.* ("DOJ's data transfer policies already follow this core principle and provide personally identifying data only in cases where it is necessary to conduct the research"). But for other projects that cannot be conducted without individual-level data, the court accepted DOJ's assertion that anonymization or de-identification is not feasible or effective because it would impact the efficacy of the desired research—namely, the researchers would not be able to "link" firearms owners to other databases so they can "follow" their behavior for many years. *Id.* at 39–40. In short, Plaintiffs "did not provide evidence or argument sufficient to establish the existence of a feasible and effective alternative" at the preliminary injunction stage. *Id.* at 40.

Plaintiffs filed a petition for review with the California Supreme Court, which was denied on February 28, 2024. This Court entered an order denying the preliminary injunction on April 12, 2024.

III. LEGAL STANDARD

Summary judgment is appropriate when all the papers submitted show there is no triable issue of material fact and the moving party is entitled to judgment as a matter of law. Code Civ. Proc. § 437c(c). "A plaintiff may seek summary judgment or adjudication if he or she contends there is no defense to the entire action or to a particular claim. A plaintiff seeking summary judgment

bears the initial burden to prove each element of his or her causes of action." *People ex rel. City of Dana Point v. Holistic Health* (2013) 213 Cal.App.4th 1016, 1024 (citations omitted). Once a plaintiff meets this burden, the burden shifts to the defendant to show the existence of a triable issue of material fact as to the cause of action or a defense. Code Civ. Proc. § 437c(p)(1).

IV. ARGUMENT

"Unlike the federal Constitution, the California Constitution expressly recognizes a right to privacy." *Mathews v. Becerra* (2019) 8 Cal.5th 756, 768. In 1972, California voters passed the Privacy Initiative, which added "privacy" to the enumerated rights set forth in Article I, Section 1 of the California Constitution. In *Lewis v. Superior Court*, the California Supreme Court recounted the "principal 'mischiefs' that the Privacy Initiative addressed" in language that bears heavily on this case; those mischiefs included: "(1) 'government snooping' and the secret gathering of personal information; (2) the overbroad collection and retention of unnecessary personal information by government and business interests; [and] (3) the improper use of information properly obtained for a specific purpose" which is then used "for another purpose" or "disclos[ed] . . . to some third party." (2017) 3 Cal.5th 561, 569 (citation omitted). Central to the right of privacy "is the ability to control circulation of personal information." *Mathews*, 8 Cal.5th at 769 (citation omitted).

The California Supreme Court set the current framework for litigating a constitutional privacy claim in *Hill*. Under *Hill*, a privacy claim involves three essential elements: (1) the claimant must possess a legally protected privacy interest; (2) the claimant's expectation of privacy must be objectively reasonable; and (3) the invasion of privacy complained of must be serious in both its nature and scope. 7 Cal.4th at 35–37. If a plaintiff satisfies this threshold inquiry, a court applies a general balancing test. The intruder can prove "that the invasion of privacy is justified because it substantively furthers one or more countervailing interests." *Id.* at 40. The plaintiff can then "rebut a defendant's assertion of countervailing interests by showing there are feasible and effective alternatives to defendant's conduct which have a lesser impact on privacy interests." *Id.*; *see also Williams v. Super. Ct.* (2017) 3 Cal.5th 531, 552 (explaining that "the party seeking information may raise in response whatever legitimate and important countervailing interests disclosure serves, while

the party seeking protection may identify feasible alternatives that serve the same interests or protective measures that would diminish the loss of privacy").

A. DOJ's Disclosure Of Plaintiffs' PII Satisfies *Hill*'s Threshold Elements For A Constitutional Privacy Violation.

The Court of Appeal expressly declined to consider whether Plaintiffs satisfied *Hill*'s threshold factors, Slip Op. at 25–26, and decided the preliminary injunction appeal on the balancing test alone. Because this case will likely be the subject of a further appeal, the Court should address each of *Hill*'s factors in resolving the parties' competing motions for summary judgment.

1. Plaintiffs Have A Legally Protected Privacy Interest In The PII Collected In AFS and the Ammunition Purchase Records File.

Plaintiffs have a protected privacy interest in the information collected in AFS and Ammunition Purchase Records File, which includes detailed information about individuals, including their fingerprints, home addresses, phone numbers, driver license information, and other identifying information—all of this along with comprehensive firearm and ammunition purchase-and-transfer history. The California Supreme Court has long recognized that individuals have a legally protected privacy interest in even a modest subset of this information. *Cnty. of Los Angeles v. Los Angeles Cnty. Emp. Relations Comm'n* (2013) 56 Cal.4th 905, 927 (recognizing that individuals "have a legally protected privacy interest in their home addresses and telephone numbers" and "a substantial interest in the privacy of their home").

2. Plaintiffs Have A Reasonable Expectation Of Privacy In Their PII Transmitted To DOJ For Law Enforcement Purposes.

Plaintiffs have an objectively reasonable expectation of privacy in the PII they must turn over to DOJ for confidential storage in AFS and the Ammunition Purchase Records File. Individuals purchasing or transferring firearms and ammunition had a reasonable expectation that the information provided to and collected by DOJ in the course of a transaction would not be disclosed outside the government or used for non-law-enforcement purposes. AFS includes a wealth of information that most Californians undoubtedly consider highly personal (like fingerprints, home addresses, and driver license numbers). But AFS goes beyond just capturing a snapshot of such

personal information, it represents a compilation of information over time: An individual's AFS record contains their entire history of firearm and ammunition transactions—so disclosure also reveals the subject's past addresses and, to a certain extent, their associations (by showing the personal information of every person who engaged in a firearm or ammunition transaction with the subject).

Under *Hill*, a "privacy claimant must possess a reasonable expectation of privacy under the particular circumstances," and a "'reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms." *Pioneer Elecs. (USA), Inc. v. Super. Ct.* (2007) 40 Cal.4th 360, 370–71 (quoting *Hill*, 7 Cal.4th at 36, 37). "The reasonableness of a privacy expectation depends on the surrounding context," and "'customs, practices, and physical settings surrounding particular activities may create or inhibit reasonable expectations of privacy.'" *Cnty. of Los Angeles*, 56 Cal. 4th at 927 (quoting *Hill*, 7 Cal.4th at 36). And "the presence or absence of opportunities to consent voluntarily to activities impacting privacy interests obviously affects the expectations of the participant." *Hill*, 7 Cal.4th at 37. Finally, the California Supreme Court has observed that, while a longstanding practice of disclosure may diminish an expectation of privacy where such practice "was clear and served to put individuals on notice," the Court has "never held that the existence of a long-standing practice or requirement of disclosure can, by itself, defeat a reasonable expectation of privacy in the circumstances." *Mathews*, 8 Cal.5th at 777–78.

a. The California Supreme Court's Decisions Show The Reasonableness Bar Is Low When It Comes To Sharing PII.

Three of the California Supreme Court's leading privacy cases permitting the disclosure of personal contact information offer a useful contrast to AB 173's mandatory disclosure-for-research regime. The first is *Pioneer Electronics*, where the Court considered the discoverability of nonparty contact information in a consumer class action case. 40 Cal.4th 360. Plaintiffs sought discovery of other customers who had filed complaints with the company about defective DVD players. *Id.* at 363–65. The Court concluded that, under the circumstances, the complaining customers did not have a reasonable expectation that their information would be shielded from discovery in the class action absent their affirmative consent:

> Pioneer's complaining customers might reasonably expect to be notified of, and given an opportunity to object to, the release of their identifying information to third persons. Yet it seems unlikely that these customers, having already voluntarily disclosed their identifying information to that company in the hope of obtaining some form of relief, would have a reasonable expectation that such information would be kept private and withheld from a class action plaintiff who possibly seeks similar relief for other Pioneer customers, *unless the customer expressly consented to such disclosure.* If anything, these complainants might reasonably expect, and even hope, that their names and addresses would be given to any such class action plaintiff.

Id. at 372 (italics in original).

Next, in *County of Los Angeles*, the Court considered the disclosure of public employees' contact information to a public employee union that the employees had refused to join. 56 Cal.4th 905. After concluding that "home contact information is generally considered private," the Court held that nonmembers had a reasonable but "reduced" expectation of privacy because of the "common practice" of public employers to share contact information with unions in particular circumstances. *Id.* at 927, 928–29. The Court observed that nonmembers provided their information "for the limited purpose of securing employment," and therefore could "reasonably expect that the employer will not divulge the information outside the entity except in very limited circumstances." *Id.* at 927–28; *see id.* at 928 (noting that employers may be required to share contact information with government agencies or to "banks or insurance companies" concerning employee benefits).[9] The Court also remarked that the disclosure posed a "more significant privacy invasion" than in *Pioneer* because nonmembers had "chosen not to join [the union] and have declined in the past to give their contact information." *Id.* at 930; *see also id.* (highlighting the notice and opt-out procedure in *Pioneer* that "mitigated any privacy invasion").

Finally, in *Williams* the Court extended *Pioneer*'s logic to permit discovery of employee contact information in wage-and-hour class action cases, concluding that employees did not have a reasonable expectation that their home contact information would not be shared in that particular

[9] The Court ultimately held that the union's duty of fair representation to all employees (including nonmembers) justified the privacy invasion because direct communication with nonmembers was essential. *Cnty. of Los Angeles*, 56 Cal.4th at 931. Following *Pioneer*, the Court assumed that sharing nonmembers' contact information with the union promoted their interests, while nonmembers suffered only a "mild" privacy intrusion based on the "common practice of disclosure [of home contact information to unions] in other settings." *Id.* at 932. But the Court was careful to highlight that the "balance might, in some cases, tip in favor of privacy when an individual employee objects and demands that home contact information be withheld." *Id.* at 932.

context. 3 Cal.5th at 554–55. The Court acknowledged that "absent employees have a bona fide interest in the confidentiality of their contact information," but then stressed that, as in *Pioneer*, it was unlikely that "employees would expect that information to be withheld from a plaintiff seeking to prove labor law violations committed against them and to recover civil penalties on their behalf." *Id.* at 554. In other words, it was objectively reasonable to conclude that people don't expect their contact information to be kept private when disclosure enhanced the opportunity for them to recover money.

b. Plaintiffs Easily Satisfy The Low Reasonableness Bar.

The principles in these cases cut precisely the opposite way here to confirm that Plaintiffs' expectation of privacy in far more than just their contact information is objectively reasonable. Unlike a consumer who complained about a defective product and stood to gain in a consumer class action, or an aggrieved employee who might profit from class-action litigation, the circumstances here show that gun owners would not possibly have an expectation that their private data would be shared with these research institutions. Disclosure does not directly benefit them (as in a class action setting like *Pioneer* and *Williams*, or in a collective bargaining setting like *County of Los Angeles*); disclosure is being made for a purpose different from why it was collected; and in any event, there is zero basis in law or logic to think that firearm owners would expect their confidential data would be used to make them research subjects to promote reduced access to firearms. Plaintiffs obviously have a reasonable expectation that their private information would not be disclosed in these circumstances.

Beyond these big-picture points, the reasonableness of Plaintiffs' expectation that their private information will be kept private by DOJ is confirmed by 25 years of assurances in Penal Code section 11106 that their data would, in fact, be kept confidential by DOJ and could only be shared within the government for law enforcement purposes only. DOJ itself doubled down on these assurances in their privacy disclosures. This expectation was bolstered by the voters' enactment of Proposition 63 in 2016, which explicitly provided that personal information collected by DOJ for ammunition transactions "shall remain confidential and may be used . . . only for law enforcement purposes." Penal Code § 30352(b)(2). This "long-standing and consistent practice" restricting the

use of PII collected for firearm and ammunition transactions to law enforcement purposes supports Plaintiffs' reasonable expectation that their information would *not* be used for unrelated purposes. *Cnty. of Los Angeles*, 56 Cal.4th at 927–28.

And the fact that Plaintiffs were given no notice or opportunity to consent or refuse before their PII was shared with researchers further underscores the reasonableness of their expectation. *See Hill*, 7 Cal.4th at 37 (the "presence or absence of opportunities to consent voluntarily" affects privacy expectations). Notice and consent are key to ameliorating privacy concerns and provide context to evaluate privacy expectations in a given setting. *See, e.g.*, *Pioneer*, 40 Cal.4th at 372 (evaluating consumers' privacy expectations and observing that "complaining customers might reasonably expect to be notified of, and given an opportunity to object to, the release of their identifying information to third persons"); *Cnty. Of Los Angeles*, 56 Cal.4th at 930 (highlighting the notice and opt-out procedure in *Pioneer* that "mitigated any privacy invasion"); *id.* at 932 (noting that the privacy balance might tip against disclosure "when an individual employee objects and demands that home contact information be withheld"). But here, there were no safeguards in place to provide affected individuals of notice that their PII would be shared, let alone an opportunity to consent or object. This fact heightens Plaintiffs' expectation of privacy in a setting where the government requires the submission of PII as a condition on exercising a constitutionally protected right.

In sum, case law, the statutory structure preceding AB 173, the lack of notice and opportunity to consent, and the drastically different use of the data compared to the purpose for which it was collected all confirm that Plaintiffs have a reasonable expectation of privacy in their PII.

3. Sharing PII In AFS And The Ammunition Purchase Records File Is A Serious Invasion Of Plaintiffs' Privacy.

AB 173 mandates a serious privacy invasion. Researchers now get access to PII that they actively use, mine, manipulate, and link to other databases to develop dossiers about gun owners—and then "follow" them for years. Strangers at the Center—and other "bona fide" researchers—will now know intimate details about millions of law-abiding Californians who were given no advance notice that their personal information would be used to make them research subjects; to the contrary,

they were assured by California law that their private information could only be used for law enforcement purposes. Adding insult to injury, the lack of advance notice is paired with no opportunity to opt out.

Several reasons confirm that this is a serious privacy invasion. First, the "seriousness" "'element is intended simply to screen out intrusions on privacy that are de minimis or insignificant.'" *Am. Academy of Pediatrics v. Lungren* (1997) 16 Cal.4th 307, 339 (plurality op. of George, C.J.) (citation omitted); *Lewis*, 3 Cal.5th at 571 (same). *Hill*'s "elements do not eliminate the necessity for weighing and balancing the justification for the conduct in question against the intrusion on privacy resulting from the conduct in any case that raises a genuine, *nontrivial* invasion of a protected privacy interest." *Sheehan v. San Francisco 49ers, Ltd.* (2009) 45 Cal.4th 992, 999 (citation omitted) (emphasis added). For the many reasons shown above, Plaintiffs' interest in shielding disclosure to the social science researchers here cannot possibly be dismissed as de minimis or "trivial."

The voters' decision to enshrine the right to privacy in the constitution was motivated by concerns about the precise type of disclosure Plaintiffs are subject to here. The Privacy Initiative's proponents were attuned to the unique harm arising from the government's compilation of personal information. "The proliferation of government snooping and data collecting is threatening to destroy our traditional freedoms. Government agencies seem to be competing to compile the most extensive sets of dossiers of American Citizens." *White v. Davis* (1975) 13 Cal.3d 757, 774 (quoting ballot argument). Even then, Californians recognized that technology compounded the threat to privacy: "Computerization of records makes it possible to create 'cradle-to-grave' profiles of every American." *Id.*; *see also Whalen v. Roe* (1977) 429 U.S. 589, 605 (acknowledging "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files").

And while DOJ's initial disclosure of PII is a privacy violation, the constitutional violation is not simply "complete" at the moment the data is sent. Plaintiffs are suffering an ongoing privacy violation so long as researchers use PII and mine it for their projects. The researchers' active use of the data to "follow" the research subjects for years strongly confirms the "seriousness" of the privacy

invasion. Such "sophisticated analyses of curated information as to a particular person" constitutes a serious invasion of privacy. *Lewis*, 3 Cal.5th at 581 (Liu, J., joined by Kruger, J., concurring); *see also U.S. Dep't of Just. v. Reps. Comm. For Freedom of Press* (1989) 489 U.S. 749, 766, 765 (noting in the FOIA context "that a strong privacy interest inheres in the nondisclosure of compiled computerized information" because of the "power of compilations to affect personal privacy that outstrips the combined power of the bits of information contained within").

The fact that disclosing PII for "research" is a different purpose than the purpose for which the sensitive information was collected further demonstrates the magnitude of the privacy violation. State law assured firearm purchasers for 25 years that DOJ would keep the private data confidential and use it for law enforcement purposes only. This bait and switch makes the disclosure "serious." *Cf. Lewis*, 3 Cal.5th at 569; *White*, 13 Cal.3d at 774 (right of privacy "prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes"). Even when dealing solely with home contact information, the California Supreme Court has held that disclosure is a "serious" invasion of privacy when the disclosure is inconsistent with the purpose a party supplied the information in the first place and does not clearly further the party's interest. *Cnty. Of Los Angeles*, 56 Cal.4th at 929–30. The absence of notice and the opportunity to opt out only cements this conclusion. *See id.* at 930; *Pioneer*, 40 Cal.4th at 372–73.

Moreover, sharing gun owners' PII carries the prospect of unwanted contact: Contacting individuals is entirely consistent with the broad statutory mandate of "research." The California Supreme Court has recognized the "privacy interest in avoiding unwanted communication," *County of Los Angeles*, 56 Cal.4th at 927, and held that the disclosure of just contact information is sufficiently "serious" to support a constitutional claim, *id.* at 929–30 (citing and quoting *U.S. Dep't of Def. v. Fed. Labor Relations Auth.* (1994) 510 U.S. 487, 501 (non-union employees "have some nontrivial privacy interest in nondisclosure, and in avoiding the influx of union-related mail, and, perhaps, union-related telephone calls or visits, that would follow disclosure")). Indeed, in *Department of Defense*, the Supreme Court emphasized that the "privacy of the home" is disrupted

by the prospect of "unsolicited, unwanted" contact (including "calls or visits") that may "perhaps" follow from unauthorized disclosure of contact information. 510 U.S. at 500–01.

Finally, the ongoing privacy violation mandated by AB 173 is made even more serious by the fact that DOJ *still* does not disclose that PII collected in firearm and ammunition transactions will be shared with researchers. For example, DOJ updated both the *Automated Firearms System (AFS) Request for Firearm Records* and the *Personal Firearm Eligibility Check Application* in 2024 but does not disclose AB 173's information-sharing in the associated Privacy Notice. The DROS worksheet does not include a Privacy Notice. DOJ's failure in this regard violates its obligations under the Information Practices Act, which requires agencies to disclose "[a]ny known or foreseeable disclosures which may be made of the [personal] information" they collect. Civ. Code § 1798.17(g).

* * *

In sum, Plaintiffs established all three of *Hill*'s threshold factors.

B. AB 173's Information-Sharing Regime Does Not Survive The Interest-Balancing Inquiry.

Because Plaintiffs have satisfied the threshold inquiry, the Court must engage in a balancing test that weighs DOJ's asserted countervailing interest against the magnitude of the privacy invasion. "The party seeking information may raise . . . whatever legitimate and important countervailing interests disclosure serves, while the party seeking protection may identify feasible alternatives that serve the same interests or protective measures that would diminish the loss of privacy." *Williams*, 3 Cal.5th at 552. The Court then "balance[s] these competing considerations." *Id.*

The Court of Appeal's decision has narrowed this Court's consideration of the interest-balancing inquiry. Specifically, the opinion held that the State has a "legitimate countervailing interest" in "promoting research informing policy decisions aimed at preventing or reducing firearm violence." Slip Op. at 24; *see id.* at 28–29, 30–32. Plaintiffs acknowledge that this conclusion is binding as law of the case. *See Crespin v. Coye* (1994) 27 Cal.App.4th 700, 708.

That does not end the inquiry. Under *Hill*, a privacy "[p]laintiff . . . may rebut a defendant's assertion of countervailing interests by showing there are feasible and effective alternatives to

defendant's conduct which have a lesser impact on privacy interests." 7 Cal.4th at 40; *see also Williams*, 3 Cal.5th at 552 ("the party seeking protection may identify feasible alternatives that serve the same interests or protective measures that would diminish the loss of privacy"); *Lewis*, 3 Cal.5th at 574 ("evidence of less intrusive alternatives is relevant in balancing the government's interests against the privacy intrusion at issue"). Before turning to those alternatives, we emphasize that several affirmative reasons demonstrate why the interest-balancing inquiry tilts in Plaintiffs' favor. The Court of Appeal did not address these issues.

1. AB 173 Takes PII Shared For One Purpose And Requires It To Be Shared For A Different Purpose Altogether—A Purpose That Plaintiffs Actively Oppose.

The California Supreme Court stressed in *Hill* that "[t]he right of privacy . . . prevents government . . . from misusing information gathered for one purpose in order to serve other purposes." 7 Cal.4th at 17 (quoting ballot argument). That is exactly what is happening here: As shown above, DOJ collects the information in AFS and the ammunition database for use in criminal or civil investigations. *See* Penal Code §§ 11106(a)(1) (AFS information compiled "to assist in the investigation of crime, the prosecution of civil actions . . . , [and] the arrest and prosecution of criminals"); § 30352(b)(1) (ammunition records database "shall remain confidential" and "may be used . . . only for law enforcement purposes"). Yet AB 173 requires DOJ to share this information for another purpose (research) and directs DOJ to share it with private third parties for that different use. This strikes at the heart of one of the "principal mischiefs" the Privacy Initiative sought to address: "the improper use of information properly obtained for a specific purpose" and then used "for another purpose" or disclosed to "some third party." *White*, 13 Cal.3d at 775; *accord Lewis*, 3 Cal.5th at 569.

Again, compare this disclosure to the disclosures of contact information that survived the balancing tests in *Pioneer Electronics*, *County of Los Angeles*, and *Williams*. In each of those cases, the Supreme Court tolerated privacy invasions principally because they *furthered* the interests of the individuals whose data was being disclosed. *Pioneer*, 40 Cal.4th at 372 (disclosure furthered consumers' interests in resolving complaints about defective products); *Cnty. of Los Angeles*, 56 Cal.4th at 931–32 (sharing nonmembers' contact information with union promoted the employees'

interests); *Williams*, 3 Cal.5th at 553–54 (permitting discovery of employees' contact information in wage-and-hour class action that could benefit them financially). And in each case, there was a nexus between the individual and the purpose of the disclosure that reduced the magnitude of the privacy invasion (*e.g.*, a consumer or employee relationship), and the private information was either voluntarily provided or the individuals had notice and the opportunity to opt-out.

This case is radically different. The millions of gun owners in AFS have no connection whatsoever to the social scientists who want to use their PII to make them research subjects. And that use is entirely divorced from the purpose it was provided to DOJ in the first place. Whereas the Court concluded in *Pioneer* and *Williams* that the facts suggested the plaintiffs would have *wanted* their information disclosed, here the Plaintiffs actively and vigorously oppose having their confidential information used in an effort to justify limitations on firearms rights.

And of course, there are a host of subsidiary issues that mark this case as different from the limited disclosures of private information the California Supreme Court has tolerated in the past: The privacy intrusion is far more severe than sharing just contact information. There is no analogous program or other custom or practice that could have possibly caused Plaintiffs to suspect that their personal data could be disclosed for these purposes. And Plaintiffs were not notified of the potential disclosure or given the opportunity to opt out. In short, the core factors that mitigated privacy concerns in the California Supreme Court's previous cases are absent here.

2. AB 173's Privacy Intrusion Is Significant And Compounded By Researchers' Ongoing Use Of Plaintiffs' PII.

The scope of a privacy violation is significant. AFS and the Ammunition Purchase Records File contain a vast amount of detailed PII that AB 173 requires DOJ to share with outside researchers who compound the privacy violation by linking it with other data and then "following" gun owners for years. *Lewis*, 3 Cal.5th at 581 (Liu, J., joined by Kruger, J., concurring); *accord Reps. Comm. For Freedom of Press*, 489 U.S. at 765–66 (noting in the FOIA context "that a strong privacy interest inheres in the nondisclosure of compiled computerized information" because of the "power of compilations to affect personal privacy that outstrips the combined power of the bits of information

contained within"). The aggregation and compilation of PII and its subsequent use by researchers compounds the privacy violation mandated by AB 173.

3. The Government's Involvement Tilts The Scales In Plaintiffs' Favor.

The flow of information from the government to private researchers here is important. *Hill* stressed that "[j]udicial assessment of the relative strength and importance of privacy norms and countervailing interests may differ in cases of private, as opposed to government, action." 7 Cal.4th at 38. Importantly, "the pervasive presence of coercive government power in basic areas of human life typically poses greater dangers to the freedoms of the citizenry than actions by private persons." *Id*. So where, as here, "a public or private entity *controls access to a vitally necessary item*, it may have a correspondingly greater impact on the privacy rights of those with whom it deals." *Id*. at 39 (emphasis added). California conditions exercise of the fundamental constitutional right to purchase firearms on disclosing PII to DOJ—and now that data is being distributed to private researchers (opposed to the gun owners' choices) with no opportunity to consent. Plaintiffs are not "able to choose freely among competing public or private entities in obtaining access" to the exercise of this right, so *Hill* instructs that the government faces a steeper burden in the balancing test. *Id.* at 39.

4. There Are Feasible and Effective Alternatives That Would Have A Lesser Impact On Privacy Interests.

Plaintiffs have identified two specific alternatives that can minimize AB 173's intrusion on privacy interests: (1) individuals should be given notice of each data request and provided an opportunity to opt out of (or opt in to) having their information shared with researchers; and (2) DOJ could restrict sharing of PII by implementing protective procedures that anonymize or de-identify data shared with researchers. Each of these proposed alternatives is technically "feasible," as DOJ can provide notice to those in the State's databases—and to future firearm and ammunition purchasers—that their PII may be shared with researchers and give them the opportunity to opt out of (or opt in to) such sharing.[10] DOJ could also anonymize or de-identify information from the

[10] Providing notice and the opportunity to opt out of having PII shared is a straightforward alternative that is consistent with the California Supreme Court's privacy cases. *See, e.g.*, *Hill*, 7 Cal.4th at 37 (the "presence or absence of opportunities to consent voluntarily" affects privacy expectations);

database, as shown by DOJ's own researchers and expert.[11] And so far as Plaintiffs are concerned, each of these alternatives are "effective," in that either alternative would in fact "have a lesser impact" on their privacy interests. *Hill,* 7 Cal. 4th at 40. The identification of such alternatives is sufficient to meet Plaintiffs' affirmative burden on summary judgment.

DOJ is expected to argue in response that these alternatives are neither feasible nor effective. To that end, DOJ has represented to Plaintiffs that it intends to support its cross-motion for summary judgment with supplemental declarations from (at least) Professor Wintemute and Professor Studdert. In light of the Court of Appeal's decision on this issue, *see* Slip Op. at 35–41, the parties have agreed to defer depositions of Professors Wintemute and Studdert until after DOJ files its first summary judgment brief. Plaintiffs will therefore address the issue of "feasible" and "effective" alternative courses of conduct in further detail in their consolidated reply and opposition brief.

V. CONCLUSION

For the reasons set forth above, the Court should grant Plaintiffs' motion and enter judgment in their favor.

Dated: December 13, 2024

BENBROOK LAW GROUP, PC

By s/ Stephen M. Duvernay
STEPHEN M. DUVERNAY
Attorneys for Plaintiffs

Pioneer, 40 Cal.4th at 372 (evaluating consumers' privacy expectations and observing that "complaining customers might reasonably expect to be notified of, and given an opportunity to object to, the release of their identifying information to third persons"); *Cnty. Of Los Angeles*, 56 Cal.4th at 930 (highlighting the notice and opt-out procedure in Pioneer that "mitigated any privacy invasion"); *id.* at 932 (noting that the privacy balance might tip against disclosure "when an individual employee objects and demands that home contact information be withheld").

[11] This could include, for example, assigning subject codes in lieu of sharing names, driver's license or identification card numbers, or using other unique identifiers; and using higher-level geographic data (such as ZIP Codes or city- or county-level data) in lieu of home addresses. *See, e.g.*, Garfinkel, U.S. Dep't of Commerce, Nat'l Inst. of Standards & Tech., *De-Identification of Personal Information* 15–16, 19–21 (2015) (discussing methods of deidentifying structured datasets).