SENIOR PARTNER
C. D. Michel*

PARTNERS
Anna M. Barvir
Matthew D. Cubeiro
Joshua Robert Dale**
W. Lee Smith

* Also admitted in Texas and the District of Columbia
** Also admitted in Nevada

MICHEL & ASSOCIATES, P.C.
Attorneys at Law
Firearms - Environmental - Land Use - Employment Law
Civil Litigation - Criminal Defense

180 East Ocean Boulevard • Suite 200
Long Beach • California • 90802
562-216-4444 • www.michellawyers.com

ASSOCIATES
Tiffany D. Cheuvront
Alexander A. Frank
Konstadinos T. Moros

OF COUNSEL
Sean A. Brady
Jason A. Davis
Joseph Di Monda
Scott M. Franklin
Michael W. Price

MEMORANDUM OF LAW

From: **Michel & Associates, P.C.**
To: **Affected CCW Holders and Applicants**
Re: **Potential Claims Arising from the California DOJ's CCW Leak**
Date: **October 19, 2022**

I. INTRODUCTION

On June 27, 2022, the California Department of Justice announced the launch of a new and updated online firearms data portal, freely open to the public. DOJ touted this new web portal as a helpful information resource that would provide an interactive and easily searchable user experience.

The portal went live on June 27, 2022, viewable at https://openjustice.doj.ca.gov/. The claimed purpose of the portal was to facilitate public access to data about various categories of firearm records, including concealed carry weapon permits and gun violence restraining orders. However, the portal went live with a significant flaw: it allowed the general public to download data that included personally identifiable and private information of thousands of California Concealed Carry Weapons (CCW) permit holders and other firearms information. This trove of data even included the home address of public officials like judges, prosecutors, reserve police officers, and correctional officers, which information is generally kept private due to safety concerns.

II. THE LEAKED CONFIDENTIAL INFORMATION

The DOJ has not as of yet identified what specific information was leaked. However, a review of leaked data culled by users of the portal confirm that the following information was included in the leaked spreadsheet documents:

1) **CCW record information for all CCW licenses applied for or issued between 2011 through 2021 including:**
    a. The CCW license holder's or applicant's name;
    b. Address;
    c. Date of birth;
    d. Gender;
    e. CCW License Number;
    f. Issue dates of license;
    g. Criminal Identification and Information (CII) Number;
    h. Type of CCW license ("judge," "custodial officer," "reserve officer," "place of employment," or "standard"); and
    i. Status of license.

2) **Firearm Safety Certificate (FSC) record information containing:**
    a. The FSC holder's date of birth;
    b. FSC holder identification number;
    c. California Driver's License Number; and
    d. Date of issuance of the FSC.

    This spreadsheet did not include names.

3) **"Assault weapon" registration information including:**
    a. The county of residence of the registrant;
    b. Date of birth;
    c. Gender;
    d. Firearm type and model;
    e. AW Registration Number; and
    f. Status of registration.

    This spreadsheet did not include names.

4) **Dealer Record of Sale (DROS) information for over 1,000,000 transactions including:**
    a. The buyer's date of birth;

b. Race;
c. Gender;
d. Whether the firearm transferred was new or used;
e. Date of the transaction;
f. Firearm type, make, and model;
g. Transaction type ("dealer sale" "non-roster peace officer transfer," "private party transfer" "pawn redemption," "storage return," or "curio and relic transfer");
h. California FFL License Number of dealer; and
i. Originating Agency Identifier (ORI) Number.

This spreadsheet did not include names.

5) **Gun Violence Restraining Order information for roughly 1,185 GVRO requests, including:**
   a. County of issuance;
   b. Year of issuance;
   c. Classification of the requestor ("family," employer," "coworker," "school," or "law enforcement"); and
   d. Procedural classification of the order issued ("emergency," "temporary," or "order after hearing").

   This database did not include names.

Of all these categories of data breaches, the CCW data breach appears to be the most serious because it includes the names and addresses of individual license holders. The other data categories described above do not appear to include name or specific address identification information, however, given other personal information included in those databases (e.g., date of birth combined with gender, race, and/or county of residence), there is a likelihood that someone could use such information in conjunction with online databases like Lexis to identify an individual by name and address.

As of the morning of June 28th, it was unclear if the data remained available or if it has been permanently removed from the state's webpages. Later in the day on June 28th, the portal through which the information was available was shut down and an error message replaced the webpage.

III. ANALYSIS OF PRIVACY LAWS UNDER WHICH THE DOJ DATA LEAK COULD BE PURSUED

California law treats information privacy seriously. The following sections describe the plausible civil claim theories against the DOJ for the data leak. The claims analyzed include those arising under the federal constitutional right to privacy, the state constitutional right to privacy and claims arising under state statutes.

A. Federal Right to Privacy for an Intentional Leak: 14th Amendment to the U.S. Constitution & 42 U.S.C. § 1983

A claim brought under Section 1983 based on the federal right to privacy is a tenuous theory of liability. Unless more information as to the reason for the leak is revealed which shows the leak to have been an intentional act (i.e., the person or persons at the DOJ who caused or facilitated the leak did so with the intent to publish gun owners' personal information), a Section 1983 action based on a *negligent* leak of the data would be unsuccessful.

The legal reason why is that "negligent conduct by a state official, even though causing injury" is not grounds for finding the deprivation of a constitutional right. *Daniels v. Williams*, 474 U.S. 327, 331 (1986). However, in the event there is evidence of intentionality, the analysis would be shaped by the following factors and issues.

While the federal right to privacy is more of a civil rights theory for invalidating laws that intrude into the domain of private individual affairs, there is also a weight of authority that recognizes "the individual interest in avoiding disclosure of personal matters." *Whalen v. Roe*, 429 U.S. 589, 599 (1977). "[I]nformation may be classified as 'private' if it is 'intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public.'" *U.S. Dep't of Just. v. Reps. Comm. For Freedom of Press*, 489 U.S. 749, 763 (1989) (citation omitted). This "informational privacy" interest "applies both when an individual chooses not to disclose highly sensitive information to the government and when an individual seeks assurance that such information will not be made public." *Planned Parenthood of S. Ariz. v. Lawall,* 307 F. 3d 782, 789-90 (9th Cir. 2002).

In the Ninth Circuit, the key authority here is *Ferm v. United States Trustee (In re Crawford)*, 194 F.3d 954 (9th Cir. 1999). The plaintiff in *Crawford* sought to keep his Social Security Number off of court filings. He was a licensed bankruptcy petition preparer, not an attorney, and the law required disclosure of his Social Security Number on the forms. *Crawford* recognized that the informational privacy interest is "not absolute; rather, it is a conditional right which may be infringed upon a showing of proper government interest." *Id*. at 959, citing *Doe v.*

Attorney General, 941 F.2d 780, 795 (9th Cir. 1991). *Crawford* emphasized that the "overall context, rather than the particular item of information" is the heart of the analysis. *Id*. at 959.

As such, the relevant questions under this contextual analysis would be who the people are whose data was leaked, what privacy interest the data regards or describes, and why the interest in keeping it confidential is important. The court would essentially weigh the competing interests. *Id*. Relevant factors to consider include:

> the type of record requested, the information it does or might contain, the potential for harm in any subsequent non-consensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.

Doe v. Attorney General, 941 F.2d at 796.

Moreover, "in each case . . . the government has the burden of showing that its use of the information would advance a legitimate state interest and that its actions are narrowly tailored to meet the legitimate interest." *Crawford*, 194 F.3d at 959. This is effectively an "intermediate scrutiny" test. *See id.* at 960.

One contextual factor of importance is the relationship between the disclosure and personal safety. Although only a district court case, *Varo v. L.A. Cty. Dist. Attorney's Office*, 473 F. Supp. 3d 1066 (C.D. Cal. 2019) is illustrative here because it involved an accidental leak of information with severe safety implications. In *Varo*, a prosecutor handed a perpetrator a criminal protective order that was supposed to prevent him from approaching the victims but instead the order contained the victim's unredacted name and address information, the release of which led to the victim being attacked. *Id*. at 1069. Citing *Crawford*, the court reasoned that "the right to informational privacy may prevent the government from disclosing to a foreseeably dangerous criminal defendant the identities and the home addresses of victims, cooperating witnesses, and their relatives." *Id.* at 1075. The court reasoned that if the disclosure of social security numbers at issue in *Crawford* implicates informational privacy rights based on the attended vulnerability to identify theft then "the nonconsensual disclosure of information that exposes individuals to violent physical harm perforce implicates those same interests." *Id*.

The *Varo* court reasoned that while "the disclosure of names and addresses" may not implicate the right to informational privacy, the disclosure in the specific context at issue—disclosure which apprises a dangerous criminal of the names and addresses of people

cooperating with a prosecution's case against him—is surely enough to implicate informational privacy interests. *Id*.

So, the lesson from the *Varo* interpretation and application of *Crawford* is clear: context is everything and safety implications validate the personal privacy interest. A release of the names and addresses of everyone who drives a Honda-brand automobile, for example, probably lacks the contextual implications to warrant a reasonable informational privacy concern. But the release of the names and addresses of people who carry concealed firearms in a state where gun rights are much maligned and where many people carry because of specific concerns about their safety, is a graver context. This is particularly true given that some of the people whose name and address information were released are judges, prosecutors, and law enforcement. California has a public policy that recognizes that dissemination of these peoples' information is to be avoided due to safety concerns arising out of their law enforcement and criminal justice activities. *See., e.g.,* CAL. GOV. CODE § 6254.21(a), and *see Crawford,* 194 F.3d at 958 ("Judicial and legislative actions in other contexts also support the conclusion that the disclosure of SSNs can raise serious privacy concerns.").

Conclusion: Because negligent behavior by a state official that results in the release of private information isn't actionable under Section 1983, this cause of action is viable only if intentional conduct is shown. If intentional conduct is shown, the context of the leak—including private information about judges, prosecutors, and law enforcement officers—would likely provide sufficient context of the gravity of the leak to overcome an intermediate scrutiny analysis and allow the mater to go to a jury.

B. Right to Privacy Under Article I, Section 1 of the California Constitution

Because the right to privacy under the California state constitution is "much broader than its federal analog," the privacy claim theory under the California Constitution is less likely to be barred at the pleading stage. *American Academy of Pediatrics v. Lungren*, 16 Cal. 4th 307, 325–26 (1997). The right of privacy protects the individual's reasonable expectation of privacy against a serious invasion. *See Pioneer Elecs. (USA), Inc. v. Superior Court*, 40 Cal. 4th 360, 370 (2007).

And important to the leak by DOJ, "California courts recognize a constitutionally protected interest in a person's name, address, and phone number." *Padron v. Lara,* No. 1:16-cv-00549-SAB, 2018 U.S. Dist. LEXIS 80161, at *38 (E.D. Cal. May 11, 2018). *Padron* cites a handful of California state court decisions recognizing a cognizable privacy interest in home address information in various contexts. See *County of Los Angeles v. Los Angeles Cty.*

Employee Relations Comm., 56 Cal. 4th 905, 927-28 (2013), *Pioneer Elecs. (USA)* at 372, and *Puerto v. Superior Court (Wild Oats Markets)*, 158 Cal. App. 4th 1242, 1252 (Ct. App. 2008).

A California case involving plaintiffs claiming a privacy interest in their home address information is instructive here, *Folgelstrom v. Lamps Plus, Inc.,* 195 Cal. App. 4th 986 (Ct. App. 2011). The plaintiffs in *Folgelstrom* purchased goods from Lamps Plus. At the point of purchase, the store asked for plaintiffs' zip code info so that the store could then cross reference that data point with other data points, determine their home address, and then mail marketing materials to them. Plaintiffs alleged that violated their privacy interest in their home address.

The court began its analysis with the elements of a cause of action for violation of the California Constitution's guaranteed right to privacy: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Hill v. National Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 39-40 (1994). A cause of action for violation of the right to privacy under the California Constitution can be asserted against a governmental entity in a lawsuit by a member of the public. *See id.* at 20, and *American Acad. of Pediatrics v. Lungren*, 16 Cal. 4th 307, 322 (1997) (violation asserted in seeking declaratory and injunctive relief). *See also Faunce v. Cate,* 222 Cal. App. 4th 166, 169 (Ct. App. 2013) (prisoner sued prison officials in their individual capacities for privacy violation), *Tom v. City and Cty. of San Francisco*, 120 Cal. App. 4th 674, 679 (Ct. App. 2004) (violation asserted in writ of mandate petition). *And see Doe v. Beard,* 63 F. Supp. 3d 1159, 1169-70 (C.D. Cal. 2014) (claims asserted as a separate cause of action under federal court's supplemental jurisdiction), and *Trujillo v. City of Ontario*, 428 F. Supp. 1094, 1123-24 (C.D. Cal. 2006) (state constitutional violation brought as supplemental claim in federal Section 1983 action but dismissed due to immunity for law enforcement investigation activities under statutory immunity afforded by Government Code section 821.6), and *Richardson-Tunnell v. Schools Ins. Program for Employees (SIPE),* 157 Cal. App. 4th 1056, 1066 (Ct. App. 2007) (constitutional privacy claim against government entity was barred by statutory immunities) *overruled on other grounds in Quigley v. Garden Valley Fire Protection Dist.*, 7 Cal. 5th 798, 815 (2019).

Element (1), the legally protected privacy interest, basically imports the two federal notions: (1) interests in precluding the dissemination or misuse of sensitive and confidential information ("informational privacy"); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference ("autonomy privacy"). *Hill,* 7 Cal. 4th at 35.

A reasonable expectation of privacy (element 2) is an "objective entitlement founded on broadly based and wide accepted community norms." *Id*. For element 3, the invasion of privacy

complained of must be "serious" in the nature, scope, and actual or potential impact to constitute an "egregious" breach of social norms. *Id*.

In *Folgelstrom*, the court noted that "residential privacy interests have been recognized in a number of cases. 195 Cal. App. 4th at 990. But the nature of the intrusion must be "serious." *Id.* at 992. "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *Hill,* 7 Cal. 4th at 37.

"Here, the supposed invasion of privacy essentially consisted of Lamps Plus obtaining plaintiffs' address without their knowledge or permission, and using it to mail coupons and other advertisements. This conduct is not an egregious breach of social norms, but routine commercial behavior." *Folgelstrom* at 992. As such, *Folgelstrom* shows that there is no per se standard of protection for address privacy. The contextual seriousness is what's important, and therefore, a plaintiff must identify a more serious reason why the disclosure is an invasion of privacy.

The situation with the DOJ data leak here is arguably more serious. This data leak "outs" people as concealed firearms carriers and also provides their home addresses. By definition, concealed carry is something meant to be clandestine and without anyone's knowledge. But this leak directly compromises the clandestine nature of it and exposes people to the hostility that pro-gun rights people in California may reasonable expect.

Arguably, the average CCW license holder has security interests that are compromised by the release to the general public of the fact that these folks are CCW license holders and where to find them. But in the case of uniquely situated people like those who have CCW licenses because of stalkers or other specific threats, and also for judges, prosecutors, and law enforcement officers, the security interest can be argued to be even more "serious" and constitute an "egregious breach of social norms" underlying the privacy protections for such protected individuals. *See Folgelstrom,* 195 Cal. App. 4th at 992; and *Hill,* 7 Cal. 4th at 37.

Again, California Government Code section 6254.21(a)'s prohibition against release of public officials' information provides one basis for arguing that the leak is an egregious breach of the social norms underlying the privacy protections afforded under that statute. Similarly, as to the members of the general public who are CCW license holders whose information was released, California's Information Privacy Act, Civil Code section 1798, et seq., would provide another basis for arguing that the DOJ's data leak has breached the social norms underlying those privacy protections for non-public official CCW license holders.

As to the procedure for bringing a claim against a state entity based upon a violation of the constitutional right to privacy, case law is clear that a private cause of action may be brought

for declaratory and injunctive relief—including in a writ of mandate—but is less clear that monetary damages can be recovered. *See Hill,* 7 Cal. 4th at 20, *American Acad. of Pediatrics* at 322, and *Tom* at 679.

At least two federal courts have recognized that an individual can bring a state-based cause of action for violation of the state constitutional right to privacy. See *Trujillo* at 1123-24, and *Doe v. Beard* at 1169-70. In *Trujillo*, however, the court found that the investigative qualified immunity afforded under Government Code section 821.6 shielded the particular government actors in that instance from liability for their violation of plaintiffs' privacy rights. *See Trujillo* at 1125.

In *Doe v. Beard*, the court found that governmental immunities under Government Code section 810, et seq. do not trump claims for state constitutional violations, and thus allowed a plaintiff's private cause of action for damages to proceed against a government actor for a violation of that plaintiff's right of privacy under the California Constitution. *See Doe v. Beard* at 1169. In doing so, it expressly refused to recognize or apply the holding of *Richardson-Tunnell v. Schools Ins. Program for Employees (SIPE)*, 157 Cal. App. 4th 1056 (Ct. App. 2007), which had held that a constitutional privacy claim against a government entity was barred by statutory immunities under Government Code section 810, et seq. *See Doe v. Beard* at 1170.

Assuming a claim for more than merely injunctive and declaratory relief can be maintained as part of a state court claim alleging a state constitutional violation, as to remedies, not only would damages and injunctive relief be available, but attorney's fees would also be available under California Code of Civil Procedure section 1021.5 so long as the pecuniary interest of any individual plaintiff in the case was not disproportionate in comparison to the burden of privately litigating an important public right. *See Edgerton v. State Personnel Bd.*, 83 Cal. App. 4th 1350, 1362-63 (Ct. App. 2000), and *Satrap v. Pacific Gas & Elec. Co.*, 42 Cal. App. 4th 72, 78 (Ct. App. 1996).

Conclusion: There is a colorable claim under the California Constitution's privacy standard, but the right to damages is less clear-cut if the case were brought in state court rather than in a federal court exercising supplemental jurisdiction. Additionally, some courts cases have presumed that the bringing of the cause of action requires presentment of a claim to the government agency in compliance with the Government Claims Act.

C. Right to Privacy Under California Civil Code section 1798, et seq. (the "Information Practices Act")

California's Information Practices Act (IPA) broadly protects people's interest in the confidential and private information stored in government files. CAL. CIV. CODE § 1798, et seq. Whether a claim for the DOJ's data leak is viable seemingly depends on whose privacy interest is being pursued. If the general public's privacy interest is being pursued, then there are arguable barriers to successfully bringing an IPA claim in light of relative strengths and weaknesses of the general public's privacy interest in the data that was leaked. If public officials' and law enforcement officers' privacy interest is being pursued, a claim under the IPA would seem to have a greater chance of success, for many of the same public policy reasons that make those interests stronger in pursuing federal and state constitutional violations.

The IPA provides that "all individuals have a right of privacy in information pertaining to them." CAL. CIV. CODE § 1798.1. An individual may bring an action against an agency that discloses personal information whenever that disclosure has an adverse effect on the individual. *Id.*, § 1798.45(c). The IPA's provisions are to be construed liberally so as to protect rights of privacy. *Id.,* § 1798.63.

The IPA prohibits state agencies from disclosing personal information sufficient to identify the individual to whom that information pertains unless the disclosure is permitted under one of the specific enumerated exemptions. *Id.,* § 1798.24. The IPA defines personal information as "any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual." *Id*., § 1798.3(a).

One of the specific exemptions enumerated under Section 1798.24 is when the information is asked for in the Public Records Act (PRA) request context. *Id*., § 1798.24(g). This public records act exemption is important. If any member of the public has a right to discover the information that the DOJ leaked here via a public records act request, then the DOJ's disclosure of that information to the public (whether negligent or not) isn't actionable because there is no violation of any privacy interest in that information. There's no cognizable injury.

However, the analysis does not end because the IPA provides a PRA exemption that would allow disclosure of personal identifying information. There are rules under the PRA that restrict what an agency can divulge in response to a public records act request in order to protect people's privacy. So, essentially, the IPA incorporates by reference the privacy rules of the PRA.

The key PRA statute here is Government Code section 6254(u), which specifically addresses CCW license records. That section provides: "except as provided in sections 6254.7 and 6254.13 (which do not apply here), this chapter *does not require* the disclosure of any of the following records:

> (1) Information contained in the applications for licenses to carry firearms issued pursuant to section 26150, 26155, 26170, 26215 of the Penal Code by the sheriff of a county or the chief or other head of a municipal police department that indicates when or where the applicant is vulnerable to attack or that concerns the applicant's medical or psychological history or that of members of their family.

Notice that this subdivision does not provide that a name, by itself, or, address, by itself, is per se the kind of information that should not be disclosed. It refers to information contained in the CCW license application that indicates when or where the applicant is vulnerable to attack. Section 6254(u) continues:

> (2) The home address and telephone number of prosecutors, public defenders, peace officers, judges, court commissioners, and magistrates that are set forth in applications for licenses to carry firearms issued pursuant to Section 26150, 26155, 26170, or 26215 of the Penal Code by the sheriff of a county or the chief or other head of a municipal police department.

This subdivision expressly states that the home address of various public officials are exempt from disclosure under the PRA. Section 6254(u) continues to identify additional public officials whose information is exempt from disclosure:

> (3) The home address and telephone number of prosecutors, public defenders, peace officers, judges, court commissioners, and magistrates that are set forth in licenses to carry firearms issued pursuant to Section 26150, 26155, 26170, or 26215 of the Penal Code by the sheriff of a county or the chief or other head of a municipal police department.

Also of notice is that while the exemption language of Section 6254 *does not require disclosure* of the categories described above, it is not a prohibition on disclosure. "[T]he exemptions from disclosure provided by section 6254 are permissive, not mandatory: They allow nondisclosure but do not prohibit disclosure." *Marken v. Santa Monica-Malibu Unified Sch.*

Dist., 202 Cal. App. 4th 1250, 1262 (Ct. App. 2012), citing *CBS v. Block*, 42 Cal. 3d 646, 652 (1986).

Because the exemptions in section 6254 are permissive, not mandatory, "[t]he Act endows the agency with discretionary authority to override the statutory exceptions when a dominating public interest favors disclosure." *CBS* at 652. Seemingly implicit in the *CBS* court's ruling is that discretion must be exercised before the privacy interest in records can be deemed insubstantial enough to yield to the public's interest in the records. But here, the DOJ's leak was likely not an exercise of discretion; it has so far been characterized by the Attorney General as a negligent release made without any exercise of discretion. Unless the Attorney General confirms the leak was in fact intentional, then there may be a valid privacy claim theory to pursue here for which Section 6254's discretionary nature would not provide the DOJ a defense.

On the other hand, the fact that there was never a discretionary determination made to release information may not be important. A court might be inclined to think that the absence of a discretionary determination might essentially be inconsequential if the privacy interest in the information isn't strong enough to counter the interest in disclosure. It's a causation issue. So, the ultimate question of whether there is a valid privacy interest in CCW licenseholders' name and address information is likely the only important question in determining whether there is a viable cause of action under the IPA.

For that analysis, the key case here is the aforementioned *CBS, Inc. v. Block*, which involved a PRA request for CCW license records issued by a county sheriff. CBS made a PRA request to inspect and copy applications submitted to and licenses issued by the Los Angeles Sheriff's Department (LASD) for CCW licenses. CBS was investigating possible abuses by authorities in their discretionary exercise of issuing CCW licenses to favored and celebrity applicants. LASD refused to honor the PRA request. CBS filed a motion for preliminary injunction to order release. The trial court ordered the release, with the proviso that the home addresses of the licensees be deleted. An appeal was taken.

The question before the court, in its own words, was "are the press and public prohibited from obtaining the information contained in the application for and the license to possess a concealed weapon under the PRA even though this information was open to public inspection from 1957-1968 and the Act did not specifically exempt this information from disclosure?" *Id.* at 648.

LASD argued that its interest in not disclosing the records was permitted under a catchall section of the PRA, Section 6255, which permits the agency to withhold a record if it can demonstrate that "on the facts of a particular case the public interest served by not making the

record public clearly outweighs the public interest served by disclosure of the record." *Id*. at 652.

LASD argued that releasing the info would allow "would-be attackers to more carefully plan their crime against licensees" and "will deter those who need a license from making an application." *Id*. But the court rejected these two arguments as "conjectural at best." *Ibid*. The court further reasoned that "the prospect that somehow this information in the hands of the press will increase the danger to some licensees cannot alone support a finding in favor of non-disclosure as to all. A mere assertion of possible endangerment does not "clearly outweigh" the public interest in access to these records." *Ibid.*

The court further reasoned that "the information sought here would not inflict . . . social stigma" and the information "was voluntarily given to the sheriff by the applicants." *Id.* at 654. It further reasoned that "while some of the holders of concealed weapon licenses may prefer anonymity, it is doubtful that such preferences outweigh the 'fundamental and necessary' right of the public to examine the bases upon which such licenses are issued. It is a privilege to carry a concealed weapon." *Ibid*. The court went on "furthermore, there is a clear and legislatively articulated justification for disclosure -- the right of the public and the press to review the government's conduct of its business. **Public inspection** of the **names** of license holders and the reasons the licenses were requested enables the press and the public to ensure that public officials are acting properly in issuing licenses for legitimate reasons." *Ibid*. (emphasis added).

However, the court did acknowledge that "it is possible, of course, that certain information supplied by individual applicants may under certain circumstances entail a substantial privacy interest." But it suggested that such interest would be of a medical or psychological nature. *Id*. at 655.

The court concluded by stating that the degree of subjectivity involved in granting a license made society's interest in scrutinizing even stronger. *Id.* And it noted that "further, the historical treatment of concealed weapons licenses undermines the defendants' claim that the holders have an expectation of privacy regarding such records. From 1957 to 1968, these licenses were open to public inspection pursuant to Penal Code section 12053." *Ibid*.

One important line from this case stands out near the end: "it is important to note that the Legislature did not create an exemption, express or implied, for concealed weapons licenses." This was true at the time but obviously is not true anymore. The court would very likely have been more friendly to the privacy interest in CCW license information had the exemption

provisions of subdivision (u) of Government Code section 6254 existed at the time that *CBS* was decided in 1986.[1]

So, there are a couple critical points arising from the *CBS* decision. First, it represents the premise that the public has a valid interest in knowing the names of CCW license holders, but the case can't quite be read for the proposition that addresses should be shielded from disclosure. Second, it appears that to some significant degree, *CBS's* reasoning is not all that persuasive anymore because after it was decided the Legislature amended the PRA to add a section strengthening the privacy of CCW license information. Thus, the argument to be advanced in support that the general public's CCW license name and address information is subject to protection under the IPA is that *CBS's* reasoning has been abrogated to some degree by subsequent legislative developments.

The *CBS* decision was in part supported by a 1979 California Attorney General Opinion drafted in response to an assembly member's question "are concealed weapons permit records maintained by a county sheriff subject to public inspection?" 62 Ops. Cal. Atty. Gen. 595 (1979), 1979 Cal. AG LEXIS 42. The answer was yes and no. These are the key parts of the attorney general's analysis.

The California Attorney General concluded that "the application for and record of a permit for a concealed weapon are open to public inspection unless they contain exceptional information by which a sheriff can demonstrate that the public interest served by not making such records public clearly outweighs the public interest in their disclosure as provided in section 6255 of the Government Code." *Id*. at *1.

The AG reasoned that:

> the information contained in the application and record of permit for a concealed firearm permit is essentially descriptive information needed to identify the applicant which is generally known by acquaintances and would not be the kind of information a person would normally conceal from others. At any rate we conclude that knowledge of such descriptive information would not constitute an "unwarranted" invasion of the applicant's privacy, particularly in light of the fact that for 12 years prior to 1970 Penal Code section 12053 expressly provided that the records of permits for concealed firearms were open to public inspection.

Id. at *11-*12

[1] The legislature amended Section 6254 to add the CCW license information exemption in subdivision (u) no later than 1991, perhaps earlier. Lexis has historical information for this statute only back to 1991. In 1998, the legislature amended it again to create subdivisions (1), (2), and (3). The first (u) section essentially became (u)(1).

The AG did offer the caveat that "[i]t is conceivable that in an exceptional situation the sheriff may be able to demonstrate that the public interest served by not making such records public clearly outweighs the public interest served by disclosure of the records." *Id*. at *13. But, "[a]bsent information contained in the application or record of permit for a concealed weapons permit by which the sheriff can demonstrate that the public interest served by not making such records public clearly outweighs the public interest in their disclosure pursuant to section 6255, we conclude that such records are open to public inspection under the Act." *Id*. at *14.

An unpublished case out of the U.S. District Court for the Eastern District of California is also helpful to understand the standard here, *Mehl v. Blanas*, 241 F.R.D. 653 (E.D. Cal. 2007). In *Mehl*, plaintiffs were concerned that the local sheriff was only granting CCW licenses to campaign contributors, so they sought records. The opinion is about a discovery dispute as to the scope of an order to produce CCW license records.

Defendants asked the court to modify parts of a discovery order that required the sheriff to produce CCW license applications (1) without removal of home address, Social Security Number, and other sensitive information about current and former judges, district attorneys, and police officers, and (2) without removal of information that would identify times and places the applications would be vulnerable to attack. *Id*. at 655.

Plaintiffs alleged that they needed the personal information in order to locate and depose witnesses and to determine which of them were political donors and CCW license applicants. *Id*. at 657. They alleged that privacy concerns were mitigated because the discovery order restricted the information's use to attorneys and experts' eyes only. *Ibid*.

The court reasoned "Defendants argue that the release of this sensitive information, even under the Magistrate Judge's Order, could lead to its ultimate disclosure to the public. Given the advent of the internet, were this information disclosed to the public, it would likely become widely available to anyone with a home computer." *Id*.

The court also noted that:

> disclosure of this information threatens to subject judicial and law enforcement officers to heightened risk of attacks upon themselves or their families at their place of residence and elsewhere. This threat implicates the very reason that this sensitive information is exempt from public disclosure under California law; to prevent these public servants and their families from suffering a retaliatory attack because of their constant contact with California's most violent, uncontrollable, and unpredictable residents.

Id.

This holding is about as succinct of a judicial recognition of why the privacy interest should prevail over any public interest under an IPA analysis as can be found. But it's a recognition of an interest that applies uniquely to the judges, prosecutors, and other public officials. Because of its context, it does not bolster the argument that name and address information of the general public in their CCW license information should be protected under the IPA.

The court went on to reject Plaintiff's argument that *CBS* permits disclosure of the sought confidential information. The court pointed out that the *CBS* court held that "any information on the applications and licenses that indicate the times or places where the licensee is vulnerable to attack may be deleted." *Mehl* at 657. Further, the court noted that "the *CBS* court acknowledged the interest the public has in ensuring that CCW licenses are issued impartially, but it did not address the question of the home address and other sensitive information of public servants in the criminal justice setting." *Id*. at 658.

The *Mehl* court also validated the strong privacy interest of someone who has a CCW license because of their unique exposure to threat. "In the case of a stalking or repeat domestic violence victim, revelation of times or places of vulnerability could lead the applicant's tormentor to a long sought-after opportunity to confront the applicant alone. In either case, avoiding just such a confrontation and possible tragedy is both the reason the applicant sought a CCW and the reason they have a powerful interest in keeping that information strictly confidential." *Id.* at p. 659.

To summarize, this appears to be the current state of the IPA as it relates to the leaked DOJ information:

1) Regular citizen CCW licensees:
    a. These people probably **do not** have a valid privacy interest in preventing the release of their names sufficient to outweigh the public's interest in knowing the names.

b. They probably **do** have a valid privacy interest against disclosure of their addresses.

2) Judge/Law Enforcement/similar Public Official CCW licensees:
   a. These people almost certainly **do** have a valid privacy interest in keeping their names secret.
   b. These people almost certainly **do** have a valid privacy interest in keeping their addresses secret.
3) Unusually situated citizen licensees (domestic abuse victims, etc.):
   a. These people probably **do** have a valid privacy interest in preventing the release of their names sufficient to outweigh the public's interest.
   b. These people almost certainly **do** have an interest in keeping their addresses secret as well.

Conclusion: An IPA claim will require arguing an interest balancing between the various plaintiffs' privacy interests and the public's right to know. However, even if the public has a right to know the identities of CCW licenseholders, a persuasive argument can be made that even if there is a valid public interest in knowing who has a CCW license, a CCW licenseholder's interest in their safety must prevail over the public's interest. And that interest means that address information should be/have been protected from disclosure. The argument can further be made that the in weighing the interests identified in *CBS, Inc. v.* Block, society doesn't need to know the addresses of CCW licenseholders in order for society to be able to investigate government accountability and the arbitrary exercise of government power.

Remedies:

Injunction is an available remedy. CAL. CIV. CODE § 1798.47. So are actual damages (including for mental suffering) and recovery of the costs of the action and reasonable attorney's fees are available as well. *Id*., § 1798.48. Emotional distress is one type of adverse effect subject to compensation under the IPA. *Hurley v. Department of Parks & Recreation*, 20 Cal. App. 5th 634, 649 (Cal. App. Ct. 2018). A "one-way" prevailing party attorney's fee provision requires a violating agency to reimburse a prevailing plaintiff its reasonable attorney's fees and costs. CAL. CIV. CODE § 1798.46.

The IPA also contains a provision allowing a civil action for invasion of privacy to be brought against members of the public and employees of a state agency who act in a capacity other than in their official capacity as an employee of that agency, who disseminate private information of a state agency protected under the IPA. *Id*., § 1798.53. In addition to actual

damages attorney's fees and costs, a successful plaintiff under this invasion of privacy claim can recover $2,500 in exemplary damages. The practical effect of this provision of the IPA, as it relates to the DOJ data leak, is that if the DOJ claims the leak was intentional by one of its employees, but was done in a rogue manner, then a claim could be brought against that employee.

Procedurally, filing a pre litigation government tort claim is not necessary if the only thing sought is injunctive relief. "We also recognize merit in appellant's argument that the claim is not for 'money or damages' within Government Code sections 905 and 945.4, and therefore not subject to demurrer for failure to comply with the Tort Claims Act. The notice of claim provisions do not apply to an action which seeks principally injunctive relief. . . ." *Snipes v. City of Bakersfield*, 145 Cal. App. 3d 861, 869 (Ct. App. 1983).

D. Government Code Section 6254.21 – Privacy of Appointed & Elected Officials

Judicial officers, law enforcement personnel, and prosecutors whose information was released have an additional cause of action they can assert. The release without prior specific authorization of these public officials' home addresses is specifically actionable under the Government Code section 6254.21(a): "No state or local agency shall post the home address or telephone number of any elected or appointed official on the Internet without first obtaining the written permission of that individual."

Any elected or appointed official who had their information released as part of this leak has a clear cause of action against the DOJ. This is arguably the most straightforwardly actionable aspect of the data breach.

E. Criminal Records Information

The release of individuals' CII numbers included in the CCW license data that leaked violates California Penal Code sections 11076 and 13201. There appear to be no civil enforcement mechanisms for violations of these Penal Code sections. Other than a prosecuting agency electing to criminally prosecute those people responsible for the leak, the only significance of these violations is that they reinforce arguments that release of information that violates the public policies expressed in Sections 11076 and 13201 is further evidence that the privacy interest in the information outweighs any governmental need to release the information. These further public policy violation arguments further support constitutional privacy causes of action or a cause of action under the IPA.

F. Intentional Infliction & Negligent Infliction of Emotion Distress

Generally, a public entity cannot be liable for common law torts unless there is a specific statute that authorizes that liability. CAL. GOV'T CODE § 815(a). However, a public entity may be found vicariously liable for employee's tortious acts pursuant to section 815.2, and there appears to be no statutory immunity that would bar pleading this cause of action against doe defendant DOJ employees and holding the DOJ liable. A claim for IIED would require the following elements:

1) Defendant's outrageous conduct
2) Defendant intended to cause emotional distress OR that Defendant acted with reckless disregard of the probability that emotion distress would result, knowing that the plaintiff was present when the conduct occurred
3) Suffering of emotional distress
4) Defendant's conduct was a substantial factor in causing severe emotional distress

CACI jury instructions counsel that the doctrine of *negligent* infliction of emotional distress is not actually a separate tort or cause of action from negligence. "It simply allows certain persons to recover damages for emotional distress only on a negligence cause of action even though they were not otherwise injured or harmed." (See "Directions for Use," CACI No. 1620.) Accordingly, the elements are:

1. Defendant was negligent
2. Plaintiff suffered serious emotional distress
3. Defendant's negligence was a substantial factor in causing serious emotional distress

Emotional distress includes suffering, anguish, fright horror, nervousness, grief, anxiety, worry, shock, humiliation, and shame. Serious emotional distress exists if an ordinary, reasonably person would be unable to cope with it.

CACI No. 1620.

The California Supreme Court has allowed plaintiffs to recover damages as "direct victims" in only three types of factual situations (1) the negligent mishandling of corpses, (2) the negligent misdiagnosis of a disease that could potentially harm another, and (3) the negligent breach of a duty arising out of a preexisting relationship. A preexisting relationship may exist here between the state as custodian of the private information and CCW permit holders as providers of that information. But for the state forcing people who wish to carry into a

relationship that requires people to submit personal information to the state in exchange for the permit, there would be no opportunity to have this information to harmfully disclose.

G. Public Disclosure of Private Facts

It's possible to hold a DOJ employee accountable under this tort liability theory as well. The State can be deemed liable for its employee's actions under a respondeat superior theory. The elements of a public disclosure of private facts cause of action are:

1. Defendant publicized private information concerning plaintiff
2. A reasonable person in plaintiff's position would consider the publicity highly offensive
3. Defendant knew, or acted with reckless disregard of the fact, that a reasonable person in plaintiff's position would consider the publicity highly offensive
4. The private information was not of legitimate public concern [or did not have a substantial connection to a matter of legitimate public concern]
5. Plaintiff was harmed; and
6. Defendants conduct was a substantial factor in causing plaintiff's harm

In deciding whether the information was a matter of legitimate public concern, you should consider, among other factors, the following:

(a) The social value of the information;
(b) The extent of the intrusion into plaintiff's privacy;
(c) Whether plaintiff consented to the publicity explicitly or by voluntarily seeking public attention or a public office;
(d) [Any other applicable factor]

In deciding whether defendant publicized the information, you should determine whether it was made public either by communicating it to the public at large or to so many people that the information was substantially certain to become public knowledge.

CACI No. 1801.

This cause of action seems to line up well with the facts of the controversy. The main vulnerability here may be how to define the *reasonable* person, or maybe, how to identify the reasonable person. Is it a reasonable CCW license holder, or just a reasonable average citizen? In reality, its going to be a reasonable average citizen.

The question that's going to be important here in this claim context isn't really much different from the question in the other claims – is this information sufficiently in the public's interest for it to lose protection? It's essentially a balancing test again.

This element looks at the "newsworthiness." In analyzing that element, courts try to balance the public's right to know against the plaintiff's privacy interest by drawing a protective line at the point the material revealed ceases to have any substantial connection to the subject matter of the newsworthy report. *Jackson v. Mayweather,* 10 Cal. App. 5th 1240, 1257 (Ct. App. 2017).

Here, it seems unlikely to me that any particular CCW holder's home address information "has any substantial connection" to anything that's truly newsworthy. In fact, it's absolutely reasonable to argue that the specific identities of CCW permit holders is not newsworthy information. On the other hand, the identities of people who have CCWs might arguably be a sufficiently newsworthy matter of public concern from a transparency in government licensure perspective, but specific information about where they reside doesn't seem to have that substantial connection.

It seems that post-*Bruen*, this argument may have less merit because now permits are meant to be issued to everyone who wants one. Under the old might-issue discretionary rubric pre-*Bruen*, there was a plausible argument that the identities of CCW permit holders would be probative of whether those people got CCWs because they contributed to the campaigns of the issuing authorities or otherwise had special relationships with them. But now that the standard is may issue, that rationale shouldn't apply. Which would tilt against the public's interest in the identity information.

IV. NOTIFICATION OBLIGATIONS

Regardless of the reasons for the leak, the DOJ has an immediate duty under California Civil Code section 1798.29(a) to notify in writing all of those affected by the leak.

That section provides that "[a]ny agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California" whose personal information was acquired by one or more unauthorized persons.

Based on a statement the DOJ released on June 29, 2022, they will be complying with the notification requirement: "In the coming days, the Department will notify those individuals whose data was exposed and provide additional information and resources. California law

requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person."[2]

V. CONCERNS AND FURTHER UNRESOLVED ISSUES

For claims filed based on a state constitutional privacy violation, the Government Claims Act's 6-month deadline for presenting a claim may be required to be complied with given the uncertain state of the law on the applicability of the GCA to state constitutional privacy violations seeking money. Additionally, while certain immunities like the "investigative" immunity for judicial proceedings under Government Code section 821.6 would not apply to the DOJ's data leak, other immunities may apply, again, due to the unsettled area of law regarding the application of the GCA to state constitutional violations seeking money damages. Further research into immunities under the GCA that may be deemed to apply to the circumstances of the DOJ's data leak should be researched.

Given federal courts more favorable treatment of claims of state constitutional privacy violations, including the finding that the GCA does not apply to state constitutional privacy violations, it may be more advantageous to file a state constitutional privacy violation claim in federal court rather than state court. However, such a tactic should only be considered if a viable federal constitutional privacy violation can be asserted, so as to ensure supplemental jurisdiction over the state causes of action will be exercised.

Finally, notwithstanding the several remedies identified in state and federal courts that are available, nonetheless it may be most advantageous for individual victims of the data leak to file their individual claims in a state small claims court. Such courts, which typically have a $7,500 to $10,000 monetary damages cap, may provide the best avenue for the most monetary relief than either a mass action or a class action based on the legal theories identified above.

[2] https://oag.ca.gov/news/press-releases/california-department-justice-alerts-individuals-impacted-exposure-personal

For Further Assistance:

Michel & Associates, P.C. has the largest and most experienced firearms law practice in California, but it is also a full-service law firm. We appreciate *all* of your legal business inquires and client referrals for all types of legal work. This business helps support the many pro bono public services Michel & Associates, P.C. provides on behalf of your right to keep and bear arms.

Request a free case evaluation http://michellawyers.com/free-case-evaluation/. If you have questions or concerns regarding your legal obligations, we offer a free consultation. Contact us at helpdesk@michellawyers.com.

#michellawyers.com#