THE INTERPLAY BETWEEN THE DRIVERS PRIVACY PROTECTION ACT, THE PUBLIC RECORDS LAW AND *SENNE V. VILLAGE OF PALATINE*

Remzy D. Bitar
Timothy M. Johnson
Crivello Carlson, S.C.
Phone: (414) 271-7722
rbitar@crivellocarlson.com
tjohnson@crivellocarlson.com

April 23, 2015

I. INTRODUCTION

A. Several recent developments have led to renewed interest, particularly by law enforcement agencies, in the interplay between Wisconsin's public records law and the federal Drivers Privacy Protection Act (DPPA) governing "personal information" and "highly restricted personal information" from the State Department of Motor Vehicles (DMV). This outline is intended to provide an overview of the issues and useful resources. Further clarification will hopefully be forthcoming by the courts.

B. For instance, law enforcement agencies have been requested by newspapers via open records requests to produce copies of accident and incident reports without redacting personal information or highly restricted personal information. As another example, some requesters seek such information for solicitation or for use in anticipated litigation. Many law enforcement agencies formerly produced this information. However, some are now considering implementation of a policy redacting information like names, addresses and dates of births. Such redactions are being considered under new authority (***Senne***, discussed below) interpreting the DPPA, yet some requesters are threatening potential claims for noncompliance with Wisconsin's public records law.

C. The following options are being considered or implemented in an effort to address the growing issues that may arise when the source of "personal information" or "highly restricted personal information" is the DMV, as opposed to some other source (see VIIIA):

1. Some municipalities, agencies and officials have taken one position that the DPPA is not triggered where this information is derived from some non-DMV source or where the DMV's information is simply being used for verification purposes.

2. Some municipalities, agencies and officials have taken a second position that the Attorney General's 2008 informal opinion authorizes disclosure of this information. Under this view, the belief is that the informal opinion insulates

against liability and that their policies and practices should remain the same (i.e., while there may be other public interest reasons for nondisclosure, the DPPA by itself does not prohibit the disclosure of this information). Others view this position as risky under ***Senne*** because the Attorney General (and courts) has not revisited whether the informal opinion is in harmony with ***Senne***.

3. Some municipalities, agencies and officials have taken a third position that, depending on the nature of the requester or the request, certain information may be disclosed pursuant to the exception under the DPPA "for any other use specifically authorized under the law of the State that holds the record, if such use is related to the operation of a motor vehicle or public safety." Under this position, there is disclosure of personal information but not highly restricted personal information. Others view this position as uncertain without guidance from the Attorney General or courts as to the scope and operation of this exception.

4. Some municipalities, agencies and officials have taken another position that ***Senne*** requires redaction of personal information and highly restricted personal information. Under this position, some are redacting information like addresses, driver's license numbers, social security numbers, medical information, dates of birth and sometimes even names. Under this position, the extent of redaction may depend on the Public Records Law "balancing test" in which the interests of disclosure are weighed against the interests of nondisclosure. Others view this position as an over-reaction to the ***Senne*** decision where an applicable DPPA exception can be found. Indeed, the Seventh Circuit remanded ***Senne*** to the trial court for further development and consideration of the applicable DPPA exceptions, specifically whether the information *was used* by any law enforcement agency "in carrying out its functions" or in connection with any civil or administrative proceeding.

5. Some municipalities, agencies and officials have taken yet another position that the DPPA does not reach new records created by local law enforcement that may contain such information obtained from the DMV. Others view this position as inconsistent with 18 U.S.C. § 2721(c)'s provisions governing when a "recipient" of information from the DMV may "redisclose" personal information.

D. Policies and controls should be put in place by which municipalities, agencies and officials evaluate what information is being taken from the DMV, tracking when it is being taken and by whom, how it is being used, whether the information can be obtained elsewhere, and whether it could be subject to an applicable DPPA exception. Monitoring and tracking each access of the information may help establish a record that can be used to rebut claims that the information was accessed without a permissible purpose.

These policies and controls may not be universal across all situations given the myriad circumstances involving requests for this kind of information, who uses it, how it is used and whether the nature of the request/requester yields an applicable DPPA exception.

II. OVERVIEW OF THE DPPA

A. Purpose: The Drivers Privacy Protection Act (DPPA) is a federal enactment by Congress as part of the Violent Crime Control and Law Enforcement Act of 1994. Its enactment was spurred by the 1989 murder of burgeoning actress Rebecca Schaeffer. An obsessed fan obtained Ms. Schaeffer's address and other personal information from a private detective; the detective allegedly obtained the information from Schaeffer's California motor vehicle records.

The DPPA protects the privacy of personal information assembled by State Department of Motor Vehicles (DMVs). It sets penalties for violations and makes violators liable on a civil action to the individual to whom the released information pertains.

B. Prohibition on Drivers' Information: The DPPA prohibits the release or use by any state DMV (or any officer, employee, or contractor thereof) of personal information about an individual obtained by the department in connection with a motor vehicle record. 18 U.S.C. § 2721. The DPPA provides that "a State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity" personal information or highly restricted personal information as those terms are defined in the act.

The DPPA does not apply only to DMV employees. It also prohibits "any person" from knowingly obtaining or disclosing personal information from a motor vehicle record for any use not permitted. 18 U.S.C. § 2722.

C. 1999 Amendment Granted Drivers Additional Privacy Protection by Requiring "Express Consent": The Shelby Amendment, which took effect June 1, 2000, changed the DPPA to require that states obtain a driver's express consent before releasing any highly restricted personal information.

D. Constitutional: South Carolina challenged the DPPA arguing that the Act violated federalism. The Supreme Court upheld the constitutionality of the Act as a proper exercise of Congress' Commerce Clause authority to regulate interstate commerce. **See *Reno v. Condon*, 528 U.S. 141 (2000).**

E. Limited Preemption – Counterpart State Laws: States were required to comply with the DPPA's minimum requirements by September 1997. States may pass laws to supplement the DPPA, which sets a baseline. Some states have passed such laws; Wisconsin has not.

III. KEY PROVISIONS

A. "Personal information": "information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status."

B. "Highly restricted personal information": "an individual's photograph or image, social security number, medical or disability information."

C. ''Express consent'' means "consent in writing, including consent conveyed electronically that bears an electronic signature…"

D. DOT's Table Showing Types of Information:

Personal data elements include:	**Highly restricted data elements include:**
Driver's license or ID number	An individual's photograph
Name	Social Security Number
Address	Medical or disability information
9 digit zip code (but not 5 digit zip code)	Any signature collected under Wisconsin Statute Chapter 343 (operators' licenses)
Date of birth	Biometrics, such as fingerprints
Telephone number	

Source: http://www.dot.wisconsin.gov/drivers/privacy.htm

IV. PERMISSIBLE USES

The DPPA limits the use of a driver's motor vehicle record to certain purposes. These purposes are defined in 18 U.S.C. § 2721. The uses **in bold** may be most applicable to law enforcement agencies.

- **For use by any government agency, including any court or law enforcement agency, in carrying out its functions.**
- **Use in matters of motor vehicle safety, theft, emissions, product recalls.**
- Motor vehicle market research and surveys.
- "Legitimate" business needs in transactions initiated by the individual to verify accuracy of personal information.
- **Use in connection with a civil, criminal, administrative or arbitral proceeding.**
- Research activities and statistical reports, so long as personal information is not disclosed or used to contact individuals.
- Insurance activities.

- **Providing notice for towed or impounded vehicles.**
- **Use by licensed investigators or security service for any authorized purpose.**
- Use by private toll transportation facilities.
- In response to requests for individual records if the State has obtained express consent from the individual.
- For bulk marketing distribution if State has obtained express consent from the individual.
- **Use by any requestor where the requestor can show written consent of the individual.**
- **For any other legitimate State use if it relates to motor vehicle or public safety.**

If an individual has not given consent to the release of a motor vehicle record, the DPPA limits sharing of information once it is obtained. Information may only be shared with other approved users only for permitted uses.

V. PRIVATE CAUSE OF ACTION AND FINES AND DAMAGES

The DPPA imposes criminal fines for non-compliance and grants individuals a private right of action to enforce violations including actual and punitive damages, as well as attorney's fees.

VI. *SENNE v. VILLAGE OF PALATINE* 695 F3d 597 (7th Cir. 2012)

A. Facts: At 1:35 one morning in August 2012, a Village of Palatine, Illinois, police officer ticketed a vehicle for violating the Village's overnight parking ban. The ticket included official information such as the officer's name and badge number, the date and time, vehicle information and the offense. The ticket also included the owner's full name, address, driver's license number, date of birth, sex, height and weight. The owner sued the Village under the DPPA, on behalf of himself and other similarly situated individuals, for including the latter information. The Village filed a Motion to Dismiss.

B. Decision/Outcome: Placing a parking ticket under a windshield wiper is "disclosure" of personal information prohibited by the DPPA. The Seventh Circuit remanded the case to the district court because the disclosure may have exceeded the scope of the following three permissible exceptions to non-disclosure cited by the Village: (1) for use by a law enforcement agency in carrying out its functions [§2721(b)(1)], (2) for use in connection with matters of motor vehicle or driver safety [§2721(b)(2)], or (3) for use in connection with a civil proceeding including service of process [§2721(b)(4)].

C. The district court dismissed the lawsuit. That court accepted the Village's arguments that leaving a parking ticket under a windshield wiper was not a "disclosure." Moreover, the court found that the personal information printed on the

ticket was a permitted disclosure under three exceptions to the DPPA. This decision was again appealed.

D. **A three-judge panel of the Seventh Circuit initially affirmed** the district court's decision dismissing the suit. In an opinion written by Judge Joel M. Flaum, the court rejected the Village's argument that the ticket placement was not a disclosure of the personal information. However, the panel determined that because the ticket constituted service of process related to the parking violation, that use of the personal information was permissible under the Section 2721(b)(4) exception (noted above).

E. **The Seventh Circuit, in rehearing en banc (before all appeals court judges), reversed** the earlier panel decision. In an opinion by Judge Ripple, seven judges agreed that placement of the parking ticket was a disclosure of the personal information and that the disclosure may not fall within the scope of any of the three cited exemptions. The court ruled that the phrase "for use" at the beginning of each of the exceptions required an analysis of whether inclusion of the personal information is compatible with the exception and whether the amount and type of the personal information disclosed exceeds the scope of the exception. The opinion states that each exception must be read "with an eye toward its contribution to the 'overall statutory scheme,'" and that it is clear that the applicability of a particular exception does not automatically mean that all personal information may be released under that exception.

F. Judge Flaum's dissent, which was joined by Judges Richard A. Posner, Frank H. Easterbrook and Diane S. Sykes, agreed with the majority on the disclosure issue. But, Judge Flaum stated that "Neither the text [of the DPPA] nor the legislative history conveys Congress's intent to limit the information that may be disclosed in connection with a particular exception." Judge Flaum also emphasized that "[t]he statute offers no guidance to the judges, lawyers, and public actors who will inevitably struggle to distinguish between necessary and extraneous information." He also noted that the majority's opinion "opens municipalities up to substantial liability for incorrectly predicting" whether seemingly permissible disclosures will satisfy the court's vague "actual use" standard.

G. Judge Posner also dissented in which he found "no indication that without being able to express its intention in words Congress intended to forbid police to place personal information on a parking ticket." Like Judge Flaum, he expressed concern that the majority's opinion will expose numerous municipalities to massive liability and damages for any similar disclosures made within the DPPA's four-year statute of limitations.

H. The Village of Palatine petitioned the U.S. Supreme Court for review of the Seventh Circuit's en banc decision, but on June 24, 2013, the Supreme Court denied the petition for a *writ of certiorari* and the case was returned to the United States District Court for the Northern District of Illinois.

I. Thus, the case made its way back to the district court in which it originated. In ***Senne v. Village of Palatine*, --- F.Supp.2d ----, 2013 WL 6197092 (N.D.Ill. 2013)**, the court confirmed that placing a ticket on the windshield of a vehicle constituted a "disclosure" under the DPPA, but it held that the village's use of the motor vehicle data on the ticket was a permissible use.

While the court did not agree with all the explanations in the police chief's affidavit, it did agree with the following explanations: (1) watch commanders at police stations use the information to consider whether to void tickets claimed to have been incorrectly issued to out-of-towners; (2) the information on the tickets serves the same identification purpose during traffic stops in which the driver has no identification but does have a parking ticket. In such cases, "many times" with non-English speakers, drivers "have a parking ticket in their glove box and hand that to you immediately because they have trouble communicating."; and (3) the information helps drivers when an officer issues a ticket to the wrong person. The district court then reasoned:

> Nonetheless, Senne's arguments bring to the fore a basic question about exactly what is required for one who discloses personal information covered by the DPPA to establish that its disclosure was permissible under section 2721(b). The Seventh Circuit's decision … is less than clear regarding how a court should go about determining whether the disclosed information is actually used for the purpose stated in the statutory exception. For example, does a court evaluate the use of the information on a case-by-case basis, to see if the use in a given situation was warranted—or is a general policy justifying the use enough? Does section 2721(b) require proof that the information is *always* used for the identified purpose? Is it enough that it is sometimes used for that purpose? Or is the possibility of use for the particular purpose sufficient? Further, does the party claimed to have disclosed personal information have to establish that a permissible purpose motivated the disclosure in the first place, or is an after-the-fact justification or an incidental use sufficient?
>
> The Court believes that the correct reading is that the *ultimate* or *potential* use of personal information qualifies as acceptable use under the DPPA if it is for a permissible purpose listed in section 2721(b).
>
> **…**
>
> Another district court may have put it best when it determined that obtaining personal information for potential future acceptable use is acceptable under the DPPA: "A person buys an umbrella for use in the rain, even if the person is fortunate enough never to actually use it. A homeowner buys a fire extinguisher for use in a fire, even if there is no fire." … The court further noted that "[h]ad Congress intended § 2721(b) to require actual use—rather than only a purpose to use when appropriate—it could have said so." …
>
> This reasoning applies equally to this case. The Village does not contend that the personal information that was included on the parking ticket issued to Senne was actually used for the error correction or identification-related

purposes that [the police chief] identified. And although it is conceivable that one of the incidental purposes that [the police chief] identified—the proposition that putting a person's name and identifying information on a ticket makes it more likely the person will pay—would apply in Senne's particular situation, that is less than clear. The Village's primary justifications, however, are not ticket-specific. Rather, the Village essentially contends because personal information is useful, and actually used, in some situations involving parking tickets, its disclosure on all parking tickets is justified. When Senne contends that the Village's stated justifications are speculative, what he appears to mean is that they don't necessarily apply in any given situation, and there is no way of telling in advance the situations in which they actually will apply. Senne does not offer, however, any evidence that the Village officers do *not* sometimes use personal information printed on parking tickets to identify people driving without licenses, or that watch commanders do not use the ticket to identify its bearer and then void it.

VII. RELEASING INFORMATION FOR USE IN ANTICIPATION OF LITIGATION

A. **18 USC § 2712(b)(4)** permits the use of personal information for motor vehicle records "in connection with any civil, criminal, administrative, or arbitral proceeding including the service of process [and] investigation in anticipation of litigation."

B. **Solicitation of Clients for a Potential Lawsuit: *Maracich v. Spears*, 675 F.3d 281 (4th Cir. 2012)** The Fourth Circuit held that DPPA's litigation exception applied to lawyers' conduct in obtaining and using, without their consent, car buyers' personal information from the South Carolina DMV with the singular purpose of employing it in their investigation in anticipation of, and in connection with the prosecution of, a suit against car dealerships. It was a permissible use, because the lawyers were looking to build and bolster a case against the dealerships if their initial information from consumers proved the existence of plausibly systemic violations of the Dealers Act.

This case was appealed and the U.S. Supreme Court granted the petition for review. In ***Maracich v. Spears*, 133 S.Ct. 2191 (2013)**, the Supreme Court vacated the Fourth Circuit's decision. The court held that an attorney's solicitation of a prospective client does not fall within one of the permissible-use exceptions listed in the DPPA. Where a reasonable person could discern that the predominant purpose of obtaining, using, or disclosing the protected personal information was to initiate or propose a business transaction with a prospective client, the solicitation is not exempted under the DPPA. The court recognized the potential for the information to bring about justice by notifying class members of their rights. However, the ends did not justify the means. "To the extent the solicitation of plaintiffs can help attorneys bring a larger class action, there are alternatives that do not sacrifice an individual's privacy in his or her motor vehicle records."

The Supreme Court admitted that "close cases may arise." "For example, if the predominant purpose of a letter was not to solicit a new client, but rather to ask a

witness investigatory questions or to secure her testimony at trial," the use may not violate the DPPA. But even if the information is validly obtained, it is a violation of the DPPA to later put it to an impermissible use: "acquiring petitioners' personal information for a legitimate investigatory purpose does not entitle respondents to then use that same information to send direct solicitations."

C. ***Pichler v. UNITE*, 339 F.Supp. 2d 665 (E.D. Pa. 2004):** two unions were accused of improperly obtaining personal information from motor vehicle records as part of a campaign to organize the employees of a manufacturing company. The trial court found that the unions were liable under the DPPA. According to ***Pichler***, to show that the "use and anticipation of litigation" exception applies, the union had to prove that (1) they undertook an actual investigation, (2) at the time of the investigation, litigation appears likely, and (3) the protected information obtained during the investigation would be of "use" in the litigation. The Court of Appeals affirmed summary judgment of liability against the unions. **See *Pichler v. UNITE*, 542 F.3d 380, 395 (3rd Cir. 2008)** (agreeing with the lower court that "[t]he [DPPA] contains no language that would excuse and impermissible use merely because it was executed in conjunction with a permissible [use].").

D. ***Wemhoff v. Dist. Of Columbia*, 887 A.2d 1004, 1011-1013 (D.C. App. Ct. 2005):** "[I]f a District employee discloses personal information in the motor vehicle records for the propose of allowing solicitation of clients by private attorney, that employee arguably would be vulnerable to a lawsuit, as would be the private attorney if he used the personal information to find clients for a class action lawsuit.".

E. ***Cowan v. Ernest Codelia*, PC, 149 F.Supp.2d 68, 79 (S.D.N.Y. 2001):** The plaintiff argued that a criminal defendant's search of a prosecutor's DMV records was motivated by purely personal reasons. The Court noted that "a reasonable juror could find that the DMV searches and the subsequent sending of the envelope to [the prosecutor's] residence was not for use in connection with a criminal proceeding but rather was to threaten or harass her for personal reasons. Thus, summary judgment on [the plaintiff's] DPPA claim is inappropriate."

VIII. INTERPLAY WITH WISCONSIN'S PUBLIC RECORDS LAW

A. **Issue #1:** Does the information come from a non-DMV source? If law enforcement gets the information from some other source, such as directly from participants, witnesses or others, the DPPA may be inapplicable.

B. **Issue #2:** Does the information meet the definition of "personal information" or "highly restricted information"? If not, DPPA may be inapplicable.

C. **Issue #3:** If the DPPA is triggered, does the Public Records Law require production? If so, should the production redact certain information?

D. **Collision of Dueling Policies:** Records created and maintained by government agencies are considered public records and, as such, are generally available to all

members of the public. In an "open" society, it is important that members of the public have access to records so they know how public agencies operate. However, there are exceptions. The DPPA is one of these exceptions.

E. ***New Richmond News v. City of New Richmond*, 13-cv-272:**

The issue of the DPPA's impact on compliance with open records laws is the subject of a case filed in St. Croix County by the *New Richmond News*, a local newspaper, against the City of New Richmond on March 13, 2013. The city responded to an open records request made by the newspaper but redacted motor vehicle accident reports because it believed it was required to do so based on the language of the DPPA. Upon receiving the redacted records, the newspaper sued the city alleging a violation of open records laws, and the city removed the case to federal court.

In either the state or federal court, any decision would likely have been appealed to higher courts given the significance of the issues. On October 31, 2013, Magistrate Judge Stephen Crocker granted the newspaper's motion to remand the case back to state court. A case is only appropriate for federal court jurisdiction when disputed DPPA issues are an essential element of the plaintiff's claim. Judge Crocker reasoned that because the federal issue in the case (the application of the DPPA) "arises solely as a defense to what is a purely state law claim" (the alleged violation of Wis. Stat. §§ 19.31 and 19.35), the case should be heard by a state court. "The Newspaper's request for the information does not depend on a 'smidgeon' of federal law, but instead is grounded upon the rights conferred by Wisconsin's Public Records Law."

The Circuit Court issued a decision on March 20, 2014. The court found that the DPPA does not require the redaction of the information requested because such disclosure is permitted under § 2721(b)(1) which allows for such permissible disclosure in order to allow the city to carry out its essential functions. In addition, the disclosures would be authorized under § 2721(b)(14) which provides a broad exception for use as specifically authorized under the law of the state that holds the record, "if such use is related to the operation of a motor vehicle or public safety."

F. **Public Records Access May be Denied Where there is a Clear Statutory Exception:** "Application of other laws. Any record which is specifically exempted from disclosure by state or federal law or authorized to be exempted from disclosure by state law is exempt from disclosure under s. 19.35 (1), except that any portion of that record which contains public information is open to public inspection as provided in sub. (6)." **Wis. Stat. § 19.36(1); see also § 19.35(1)(a)** (mandating disclosure "except as otherwise provided by law...").

G. **Duty to Redact:** "If a record contains information that is subject to disclosure under s. 19.35 (1) (a) or (am) and information that is not subject to such disclosure, the authority having custody of the record shall provide the information that is subject to disclosure and delete the information that is not subject to disclosure from the record before release." **Wis. Stat. § 19.36(6).** An authority is not relieved of the duty to

redact non-disclosable portions just because the authority believes that redacting confidential information is burdensome. **See *Osborn v. Bd. of Regents*, 2002 WI 83, ¶ 16, 254 Wis.2d 266, ¶ 46, 647 N.W.2d 158**.

H. Attorney General's Informal Opinion (I—02—08): Finds the disclosure of personal information permissible under the public records law, despite the DPPA. The public records law imposes a statutory duty on law enforcement agencies to respond to public records requests. In the course of carrying out those duties, personal information obtained from the DMV may be disclosed. While the AG recognized there may be non-DPPA reasons to redact, the opinion is challenged by some as being in conflict with ***Senne***.

I. Considering *Senne* Against Attorney General's Informal Opinion:

A number of observers have considered whether the Attorney General's informal opinion needs to be reconciled with the ***Senne*** decision for some or all of the reasons below:

1. AG's analysis acknowledged the lack of guidance from the United States DOJ who exclusively administers and enforces the DPPA.

2. AG also recognized complexity of issue.

3. AG's informal opinion concludes that personal information **"<u>may</u>"** be released, not MUST.

4. AG recognized that – depending on the totality of the circumstances related to a particular request – redactions may be warranted for non-DPPA statutory, common law or balancing test reasons.

5. AG seems to have rejected narrow interpretation of DPPA's exceptions, while Seventh Circuit stresses the exceptions should be narrowly construed with an eye towards the context and purpose of the DPPA.

6. Although recognizing federal preemption under ***Reno*** (which found impermissible conflict between the DPPA and South Carolina law), the AG's informal opinion could be re-analyzed in light of ***Senne*** which implicitly emphasizes ***Reno***'s holding that the DPPA is a legitimate exercise of federal power that restricts the dissemination of information.

7. AG focused on § 2721(b)(1)'s authorization to disclose personal information for "use by any government agency … in carrying out its functions." The statute does not define the "functions" of a government agency. AG reasoned, in part, that this exception and DPPA's legislative history indicates the scope of an agency's function should not be narrowly drawn to impede the abilities of law enforcement and other government agencies to carry out their duties. This reasoning underscored the AG's emphasis on the

importance of carrying out the duties of the public records law. But, ***Senne*** stresses the DPPA's legislative history also points to privacy and crime-fighting concerns which are equally important functions of a law enforcement department and that these exceptions should be narrowly construed.

8. Even under ***Senne***, law enforcement agencies can still carry out the function of complying with the public records law through appropriate redactions and taking proper care of their records. This observation tends to counter the AG's reasoning that one of the DPPA exceptions authorizes the release of "personal information" when that release is required under the laws of the State that holds the records. **18 U.S.C. § 2721(b)(14)**. In turn, the AG observed that Wis. Stats. § 346.70(4)(f) grants the public access to accident reports (i.e., "any person may with proper care … subject to orders or regulations as the custodian thereof prescribes, examine or copy such uniform traffic accident reports …"). Some have argued that custodians have training or policies involving the non-release of records where such disclosure would violate state or federal laws or for other legitimate concerns with public safety.

9. Cases involving violations of the DPPA for impermissible uses of personal information by law enforcement officers may support re-evaluating the AG's informal opinion in light of ***Senne***. **See, e.g., *Deicher v. City of Evansville*, 545 F.3d 537, 538–41 (7th Cir. 2008)** (a jury awarded plaintiffs damages when an officer released data to a member of the public for an impermissible purpose); ***Parus v. Cator*, 399 F.Supp.2d 912 (W.D. Wis. 2005)** ("undisputed facts are sufficient to support a jury finding defendant Kroeplin obtained plaintiff's personal information from the Department of Motor Vehicles for a non-law enforcement purpose.").

10. In light of ***Senne***, the "balancing test" could be re-analyzed to consider whether it favors the redaction of "personal information." ***Senne*** and other cases, along with several Wisconsin statutes guarding privacy interests, point to potential municipal liability for releasing private information due to concerns for privacy or endangerment to a person's life or safety. There are also concerns that fostering a public perception that personal information will be released may chill individuals' disclosure of information and cooperation with law enforcement.

IX. LIABILITY CASES UNDER THE DPPA

Recently, many DPPA-related liability cases have been filed in Minnesota. This trend is probably due to a highly publicized incident in which an employee of the Minnesota DNR, John Hunt, accessed the data of private citizens 19,000 times over a 5-year period through the Minnesota Driver and Vehicle Services (DVS) database. Many of the recent cases filed in Minnesota list 50 or more Minnesota municipalities, along with Mr. Hunt, as defendants. A few of the cases have also named Wisconsin counties that border Minnesota as defendants, because those counties

occasionally have to access driver's license data via the Minnesota DVS database given their close proximity.

Therefore, the following discussion involves DPPA-related liability claims.

A. ***Deicher v. City of Evansville, Wis.*, 545 F.3d 537 (7th Cir. 2008):** In this case, Jimmy Reiners called the Evansville Police Department claiming that he needed Mary Mezera's address in order to serve papers on her regarding property that they jointly owned. Officer Christopher Jones disclosed Mezera's address to Reiners who, as it turns out, is her abusive ex-husband against whom she had a restraining order. Mezera and her new husband sued the city and Officer Jones for violation of the DPPA, and at trial, they maintained that the Police Department initiated an extensive coverup of this incident. A jury awarded them $25,000 in damages.

The plaintiffs filed a motion for a new trial on the damages and appealed when it was denied. The issue on appeal related to the date of filing of the complaint as it related to the calculation of damages. The plaintiffs wanted the jury to consider the date of the notice of claim filed with the city under Wis. Stat. § 893.80, because this notice predated the filing of the complaint and related to their allegations of a coverup. The notice of claim was central to the plaintiffs' theory that the defendants had engaged in a coverup of the DPPA violation after they received the notice of claim.

The Seventh Circuit held that the district court was allowed to take judicial notice of the date of the filing of the complaint even though the date of the complaint was never admitted into evidence. However, the district court abused its discretion by failing to provide the jury with the notice of claim date even though it was a properly admitted exhibit. Because this error was prejudicial to the plaintiffs' claim for damages, the Seventh Circuit reversed and remanded the case to the district court for a new trial on damages.

B. ***Schierts v. City of Brookfield*, 868 F.Supp.2d 818 (E.D.Wis. 2012):** Parents who had never married and who lived apart, one in Arizona and the other in Wisconsin where these events took place, got into an argument over custody of their child at a day care facility. The police were called. Although the responding officer had never met either parent before, following the dispute the officer communicated regularly with the Wisconsin parent and eventually provided her with the address of the absent father by accessing motor vehicle records through the Arizona DOT. The Arizona parent eventually found out that he was discovered because the Brookfield officer gave his information to the Wisconsin parent. The Arizona parent then sued the city and the officer under the DPPA. Contrary to the ***Nelson*** decision, above, the ***Schierts*** Court concluded that the city was liable for the officer's conduct and the court granted summary judgment to the Plaintiff against both the officer and the city on the claim of violation of the DPPA.

The ***Schierts*** Court held that the police officer acted with the apparent authority of the city when he obtained the driver's license data for an impermissible purpose, and therefore the city was vicariously liable for his DPPA violations.

C. ***Kraege v. Busalacchi*, 687 F.Supp.2d 834 (W.D.Wis. 2009):** This class action was filed against the Wisconsin Department of Transportation and the Division of Motor Vehicles. The plaintiffs alleged that the DOT and DMV disclosed their motor vehicle record data to a company that specialized in aggregating and selling consumer data over the internet. The plaintiffs brought claims under both the DPPA and 42 U.S.C. § 1983.

The plaintiffs in ***Kraege*** contended that the doctrine of sovereign immunity did not bar their suit because they were asserting claims only against defendants in their individual capacities for "knowingly" releasing driver information when they "knew, or reasonably should have known" that doing so violated plaintiffs' rights under the Act. However, the court said it was evidence from the complaint and from the relief available under the DPPA that the plaintiffs were challenging the state's policies. Therefore, the court held that the plaintiffs' suit was one against the state and not individual actors, and the defendants were entitled to sovereign immunity from the DPPA claims.

The ***Kraege*** Court also held that the plaintiffs could not use § 1983 to enforce their rights under the DPPA. Because the DPPA provides more restrictive remedies, an action cannot lie under § 1983. The court also explained that individuals cannot sue a state or agency for violation of the DPPA, because the DPPA allows only the Attorney General to address a state's violations and then only by civil penalty.

D. ***Parus v. Kroeplin*, 402 F.Supp.2d 999 (W.D. Wis. 2005):** The plaintiff alleged that a Town of Minocqua police dispatcher violated the DPPA by disclosing his information to a DNR conservation warden asking about license plate registration. Thus, the court had to decide whether a police dispatcher can violate the DPPA by relaying motor vehicle record information to a law enforcement officer who has requested the information. The court held that if it were to deem the dispatcher's disclosure a violation of the DPPA, it would result second guessing by dispatchers when they received requests for protected information that are less than routine. Therefore, the court held that the dispatcher engaged in a permissible law enforcement function when she provided plaintiff's motor vehicle record information to the DNR warden.

E. ***Rasmusson v. Chisago County*, --- F.Supp.2d ----, 2014 WL 107067 (D.Minn. 2014):** In this case, a local television reporter sued several Minnesota cities and counties alleging that they accessed her motor vehicle data on hundreds of occasions. This case is similar to many others filed in Minnesota: the plaintiffs are usually local public figures or television reporters, often attractive women, who are represented by one of a handful of law firms in the Minneapolis area. They allege that each defendant violated the DPPA and attach a list of accesses by each defendant to their complaints. Their complaints include statements about their celebrity and suggest that the reason their information was accessed was because someone was curious about them due to this celebrity.

Rasmusson is the first in this group of cases in which the court has reached a decision on early motions to dismiss filed by the defendants. In each case, the defendants generally raise the same defenses: that the plaintiff has failed to allege sufficient facts to state a plausible claim for which relief may be granted; that the statute of limitations bars the claims; claims for relief under 42 USC 1983 cannot be based on violations of the DPPA, and accessing motor vehicle data is not an invasion of privacy.

The ***Rasmusson*** Court agreed with each defense raised: it held that any claim under 1983 cannot be based on an alleged violation of DPPA, because the DPPA provides the sole remedy. The court also agreed with other Minnesota cases holding that the statute of limitations for a DPPA claim accrues at the time of access and not at the time a claimant discovers the violation. As to claims for invasion of privacy, the court held that there is no violation of the Fourth Amendment because there is no reasonable expectation to privacy of motor vehicle data. Further, the plaintiff failed to state a claim for relief under state privacy laws, because the type of information accessed was not the type of private and personal information that is required for such a claim.

F. ***Kost v. Hunt,*** **--- F.Supp.2d ----, 2013 WL 6048921 (D.Minn. 2013):** The plaintiffs in this case were two private investigators who sued 23 Minnesota cities, 7 Minnesota counties, and John Hunt under the DPPA. The court dismissed all claims and held that the statute of limitations for DPPA claims begins to run at the time the access occurred—not at the time that the claimant learned of the access. The court also held that the complaint failed to state a claim upon which relief could be granted because the complaint lacked any details or facts alleging that the various defendants accessed the information for an improper purpose.

This holding is important because many claimants argue that they should be allowed to calculate the limitations period based on when they actually learned of the allegedly illegal access. Under the ***Kost*** ruling, municipalities' exposure to liability may be argued to be limited to a specific and readily identifiable period. It also establishes that a claimant cannot simply recite empty allegations (e.g. "The Smithville Police Department impermissibly accessed my driver's license data") in an attempt to shift the burden onto the defendant to establish a permissible purpose.

G. ***Nelson v. Jesson,*** **Slip Copy, 2013 WL 5888235 (D.Minn., 2013):** In this matter, the plaintiff alleged that an employee of the Minnesota Department of Human Services accessed his driver's license information along with the information of approximately 1,100 other people in violation of the DPPA.

The defendant moved for dismissal on the basis that simply "accessing" or viewing driver's license data through computer queries on a computer screen, rather than accessing a hard copy of the information, does not constitute "obtaining," "disclosing," or "using" as required by the DPPA. The court did not accept that defense and stated that "information itself is not tangible," so a person can "obtain" information simply by viewing it.

However, the court still dismissed the plaintiff's claims because the plaintiff did not allege an impermissible purpose. Instead, the plaintiff alleged that the defendant made the information available to a specific employee (who then accessed it, much like John Hunt). But just making a database available to an employee who then acts with an impermissible purpose is not enough to prove that the employer acted with an impermissible purpose. This decision may be argued to limit an employer's exposure to liability even if a wayward employee violates the DPPA.

Finally, this decision also analyzed a claim for invasion of privacy. Many plaintiffs bring claims for invasion of privacy and violations of 42 U.S.C. § 1983 when filing a DPPA lawsuit. The ***Nelson*** Court held that accessing driver's license data does not constitute an invasion of privacy because information like a person's height, weight, date of birth, hair color, eye color, and address are not the type of highly personal information intended to be protected through privacy laws.

H. ***Dahlstrom v. Sun-Times Media, LLC,*** **Not Reported in F.Supp.2d, 2013 WL 6069267 (N.D.Ill., 2013):** In this case, Chicago Mayor Richard Daley's nephew was involved in a fight and killed another man. Because of the nephew's political connections, the incident resulted in a high-profile investigation by the Chicago Police Department involving a lineup using the nephew and several Chicago police officers as stand-ins. The *Chicago Sun-Times* ran an article scrutinizing the lineup procedure used by the police department that listed each stand-in's motor vehicle data.

The police officers whose motor vehicle data was published sued the newspaper under the DPPA. The newspaper argued that the DPPA violated its First Amendment rights because, as applied, the law would prevent it from publishing something as seemingly innocent as a person's eye color. The Seventh Circuit has already determined that, <u>on its face</u>, the DPPA does not violate the First Amendment (***see Travis v. Reno,*** **163 F.3d 1000, 1007 (7th Cir.1998)**), but the question of whether the DPPA might violate the First Amendment <u>as applied</u> had not yet been decided.

The ***Dahlstrom*** Court explained that the DPPA does not make it unlawful for a newspaper to publish truthful information, such as a police officer's eye color. Instead, the DPPA makes it unlawful to "obtain or disclose" personal information from a motor vehicle record for an impermissible purpose. If a newspaper learned that an officer has brown eyes from a source other than that officer's motor vehicle record, then it may publish that fact without violating the DPPA. But because the newspaper obtained the officers' information from their motor vehicle records without any permissible purpose, it could not use the information without violating the DPPA.

I. ***Whitaker v. Appriss, Inc.*****, 2014 WL 4536559 (N.D.Ind., September 11, 2014):** The plaintiffs were in a car accident. Police officers in Indiana complete a state standard crash report that includes personal information about the participants in an accident, including information that could be found on drivers' licenses and car

titles. Officers in Indiana and six other states use Appriss's software to complete accident reports. The public can buy individual reports or a subscription service from Appriss's website. After the accident, the plaintiffs received unsolicited letters from personal injury attorneys and a chiropractor. The plaintiffs sued Appriss for selling accident reports which contained their personal information.

Appriss filed a motion to dismiss and argued that the information used in its records came from police department records, not department of motor vehicle records. Appriss also argued that much of the information in the accident reports could have come from any number of other sources – like telephone directories, voter registration rolls, litigation records, arrest records, websites, etc. Appriss also argued that police reports will also contain information about participants in a crash who do not have department of motor vehicle records, e.g. those who have never had a driver's license.

The court advised that the DPPA protects personal information that derives from department of motor vehicle records, no matter the path that information ultimately takes to the end user. Based upon the pleading standards at the motion to dismiss stage, the motion to dismiss was denied, allowing the parties to determine where exactly the information in the Appriss reports came from. This case exemplifies the increasing reach of the DPPA to third-party vendors and contractors, like Appriss, who sell products which are likely based upon DPPA-protected information.