

United States Court of Appeals
For the Eighth Circuit

No. 14-1754

Johanna Beth McDonough

Plaintiff - Appellant

v.

Anoka County; Benton County; City of Bloomington; City of Brooklyn Center; City of Brooklyn Park; City of Burnsville; Carver County; City of Coon Rapids; Dakota County Communications Center; City of Eagan; City of Elk River; City of Eveleth; City of Fergus Falls; Goodhue County; City of Hancock; Hennepin County; City of Hopkins; City of Isanti; City of Maple Grove; City of Minneapolis; City of Minnetonka; Morrison County; City of Mound; City of Mounds View; City of New Brighton; City of New Hope; City of New Prague; City of Northfield; City of Owatonna; Ramsey County; City of Redwood Falls; Renville County; Rice County; City of Richfield; City of Rochester; City of Roseville; Sherburne County; City of St. Anthony; City of St. Paul; Stearns County; City of Wayzata; Wright County; Michael Campion, acting in his individual capacity as Commissioner of the Minnesota Department of Public Safety; Ramona Dohman, acting in her individual capacity as Commissioner of the Minnesota Department of Public Safety; John and Jane Does, (1-500) acting in their individual capacity as supervisors, officers, deputies, staff, investigators, employees or agents of the other law-enforcement agencies or Al's Auto Sales Inc.; Department of Public Safety Does, (1-30) acting in their individual capacity as officers, supervisors, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety; Entity Does, (1-50) including cities, counties, municipalities, and other entities sited in Minnesota and federal departments and agencies; City of Apple Valley; City of South St. Paul; South Lake Minnetonka Police Department

Defendants - Appellees

No. 14-1756

Brooke Nicole Bass

Plaintiff - Appellant

v.

Anoka County; Benton County; Blue Earth County; Carver County; Chisago County; Clay County; Cook County; Crow Wing County; Dakota County; Dodge County; Goodhue County; Hennepin County; Houston County; Kandiyohi County; Lyon County; McLeod County; Morrison County; Murray County; Pipestone County; Ramsey County; Rice County; Scott County; Sherburne County; Stearns County; Washington County; Wright County; City of Alexandria; City of Anoka; City of Apple Valley; City of Appleton; City of Becker; City of Bemidji; City of Big Lake; City of Blaine; City of Bloomington; City of Brooklyn Center; City of Brooklyn Park; City of Burnsville; City of Champlin; City of Cottage Grove; City of Crystal; City of Dayton; City of Eagan; City of Elk River; City of Elko New Market; City of Fairmont; City of Faribault; City of Farmington; City of Forest Lake; City of Fridley; City of Gaylord; City of Hopkins; City of Inver Grove Heights; City of Jackson; City of Jordan; City of Kasson; City of Maple Grove; City of Maplewood; City of Marshall; City of Medina; City of Minnetonka; City of Minnetrista; City of Moorhead; City of Morris; City of Mounds View; City of New Hope; City of New Ulm; City of North Mankato; City of North St. Paul; City of Oakdale; City of Osseo; City of Plymouth; City of Princeton; City of Prior Lake; City of Ramsey; City of Richfield; City of Robbinsdale; City of Rosemount; City of Roseville; City of Sartell; City of Savage; City of Shakopee; City of Slayton; City of Sleepy Eye; City of Spring Lake Park; City of St. Anthony; City of St. Cloud; City of St. Francis; City of St. Joseph; City of St. Louis Park; City of Stillwater; City of Two Harbors; City of Wayzata; City of West St. Paul; City of Winona; Michael Campion, acting in his individual capacity as Commissioner of the Minnesota Department of Public Safety; Mona Dohman, acting in her individual capacity as Commissioner of the Minnesota Department of Public Safety; John Does; Jane Does, 1-500, acting in

their individual capacity as supervisors, officers, deputies, staff, investigators, employees or agents of the other named law-enforcement agencies; Entity Does, 1-50, including cities, counties, municipalities, and other entities sited in Minnesota and federal departments and agencies; Department of Public Safety Does, 1-30, acting in their individual capacity as officers, supervisors, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety

Defendants - Appellees

No. 14-1765

Dawn Mitchell

Plaintiff - Appellant

v.

Aitkin County; City of Aitkin; Anoka County; City of Anoka; City of Arlington; Beltrami County; City of Blaine; City of Bloomington; City of Brooklyn Park; Carver County; City of Champlin; Chisago County; Cook County; City of Cottage Grove; City of Crosslake; Dakota County; Freeborn County; Hennepin County; City of Hopkins; Kandiyohi County; City of Lake Shore; City of Lakeville; City of Maple Grove; City of Maplewood; City of Marshall; County of McLeod; City of Minneapolis; City of Minnetonka; Mower County; City of Plymouth; Ramsey County; City of Red Wing; Rice County; City of Roseville; City of St. Francis; St. Louis County; City of St. Paul; Stearns County; Steele County; Wright County; Entity Does (1-50), including cities, counties, municipalities, and other entities sited in Minnesota; City of Woodbury; City of Blue Earth; City of Cannon Falls; City of Crosby; City of Edina; City of Green Isle; City of Northfield; City of Rosemount; City of Wabasha; City of White Bear Lake; John & Jane Does, 1-300

Defendants - Appellees

Brian Potocnik

Plaintiff - Appellant

v.

Anoka County; Dakota County; Hennepin County; Sherburne County; City of Apple Valley; City of Big Lake; City of Biwabik; City of Bloomington; City of Brooklyn Center; City of Brooklyn Park; City of Cambridge; City of Deephaven; City of Dilworth; City of Eagan; City of Elk River; City of Farmington; City of Gilbert; City of Golden Valley; City of Hancock; City of Hoyt Lakes; City of Lake City; City of Lakeville; City of Moorhead; City of New Hope; City of New Ulm; City of Redwood Falls; City of Rosemount; City of Virginia; City of Wells; Michael Campion, acting in his individual capacity as Commissioner of the Minnesota Department of Public Safety; Ramona Dohman, acting in her individual capacity and, in her official capacity for prospective relief only, as Commissioner of the Minnesota Department of Public Safety; John and Jane Does, (1-300) acting in their individual capacity as supervisors, officers, deputies, staff, investigators, employees or agents of the others named law-enforcement agencies; Department of Public Safety Does, (1-30) acting in their individual capacity as officers, supervisors, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety; Entity Does, (1-30) including cities, counties, municipalities

Defendants - Appellees

City of Duluth; St. Louis County; City of Minneapolis; City of St. Paul

Defendants

Appeals from United States District Court
for the District of Minnesota - Minneapolis

Submitted: March 11, 2015
Filed: August 20, 2015

Before WOLLMAN, BEAM, and COLLOTON, Circuit Judges.

WOLLMAN, Circuit Judge.

In this consolidated appeal, Brooke Nicole Bass, Johanna Beth McDonough, Dawn Mitchell, and Brian Potocnik (collectively, Drivers) challenge the dismissal of their separate actions against numerous cities, counties, and other government entities, known and unknown (collectively, Local Entities); numerous unknown law enforcement or other government personnel and supervisors, officers, deputies, staff, investigators, employees, or agents of Local Entities or other government entities in Minnesota (collectively, Law Enforcement Does); current and former Commissioners of the Minnesota Department of Public Safety (DPS) Ramona Dohman and Michael Campion (collectively, Commissioners); and various unknown officers, supervisors, staff, employees, independent contractors, and agents of DPS (collectively, DPS Does).¹ Drivers allege in their complaints that the above entities and individuals (collectively, Defendants) violated the Driver's Privacy Protection Act (DPPA or Act), 18 U.S.C. §§ 2721-2725, by accessing or disclosing Drivers' personal information from motor vehicle records without a permissible purpose.² The district courts dismissed Drivers' actions for failure to state a claim. We affirm in part, reverse in part, and remand for further proceedings.

¹All Drivers except Mitchell brought claims against Commissioners and DPS Does.

²Drivers also alleged common-law claims for invasion of privacy and violations of 42 U.S.C. § 1983 but do not appeal the dismissal of those claims.

I. Background

To obtain a driver's license or motor vehicle registration from a state motor vehicle department (DMV), individuals must disclose personal information, such as names, addresses, telephone numbers, social security numbers, medical information, vehicle descriptions, and photographs. Reno v. Condon, 528 U.S. 141, 143 (2000). Concerned over the dissemination and misuse of this personal information, Congress enacted the DPPA in 1994 to regulate the sale and disclosure of information that state DMVs collect in the process of registering and licensing drivers of motor vehicles. Maracich v. Spears, 133 S. Ct. 2191, 2195 (2013).

The DPPA prohibits state DMVs from disclosing personal information in a motor vehicle record except for uses explicitly enumerated in the statute. See 18 U.S.C. § 2721(a)-(b). “Personal information” is defined as “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.” Id. § 2725(3). As relevant here, personal information in a motor vehicle record may be disclosed by a state DMV for, among other permissible uses, “use by any government agency, including any court or law enforcement agency, in carrying out its functions,” or for use by a private person acting on behalf of a government agency in carrying out its functions. Id. § 2721(b)(1). Personal information may also be disclosed by a state DMV “[f]or use in connection with any civil, criminal, administrative, or arbitral proceeding” or for “investigation in anticipation of litigation.” Id. § 2721(b)(4). A person who “knowingly obtains, discloses or uses” an individual’s personal information, “from a motor vehicle record, for a purpose not permitted” is liable to the individual, and the court may award “actual damages, but not less than liquidated damages in the amount of \$2500,” attorney’s fees, and “punitive damages upon proof of willful or reckless disregard of the law.” Id. § 2724.

According to Drivers' allegations, DPS maintains or contributes to the Driver and Vehicle Services database and the Bureau of Criminal Apprehension database, which contain personal information from Drivers' motor vehicle records.³ Law enforcement officers, government agents, and other individuals were given passwords to access the database through an internet portal or website. During the relevant time period, the website's login page included the following admonition, or something similar: "Access to this service is for authorized personnel only conducting official business." Suspecting that law enforcement officers were accessing their information without a proper purpose, Drivers contacted DPS and requested audits detailing past accesses of their motor vehicle records. Each Driver's audit showed that his or her personal information had been accessed through the database hundreds of times, primarily through Local Entities' police departments, sheriff's offices, or other agencies.

Drivers allege that none of the Law Enforcement Does' accesses fell within the DPPA's permitted exceptions for the disclosure, use, and obtainment of personal information. Several Drivers' complaints state that the true purpose for the Law Enforcement Does' accesses was "to satisfy their shallow desires to peek behind the curtain" into Drivers' private lives. Bass and Mitchell allege that they do not have criminal records and have committed no crimes that would justify the accesses of their personal information. McDonough and Potocnik do not allege that they have no criminal records, but do allege that Law Enforcement Does obtained their personal information "without probable cause or reasonable suspicion" and that at no time did they "behave in a manner that would provide any legal justification" for the accesses. Drivers claim that their personal data was obtained through queries that used their names rather than their license plate numbers. Drivers attach as exhibits to the complaints their audits, which show the date and time of each access, as well as the

³Drivers' complaints do not always distinguish between the databases, so hereinafter we refer to either or both simply as "the database."

“source station”—*i.e.*, “the police department, sheriff’s office, or other government entity through which” Law Enforcement Does accessed the information. The audits show that government users—through the stations of different agencies, departments, branches, or other government divisions (collectively, agencies) across the state—accessed Drivers’ data during late-night or early-morning hours and often at times in close proximity to one other. Furthermore, several Drivers allege that testimony by the legislative auditor at a Minnesota Legislative Audit Subcommittee hearing in February 2013 reflects that at least fifty percent of law enforcement officers were misusing the database by accessing, using, or disclosing personal information for an impermissible purpose. McDonough, Mitchell, and Bass claim that they had had professional contact with numerous law enforcement personnel and, in some cases, a degree of local fame, which could explain Law Enforcement Does’ high level of interest in their personal information.⁴

The district courts dismissed the complaints, determining that each Driver’s allegations failed to state a claim. The district courts held that the statute of limitations began to run at the time of each alleged obtainment or disclosure of the personal data, rather than at the time Drivers became aware of the alleged violations. The district court in Bass, McDonough, and Potocnik determined that the allegations were insufficient to state a claim against the Commissioners because Drivers had not shown that “the Commissioners *themselves*” had disclosed Drivers’ personal information for an impermissible purpose. The district courts dismissed all DPPA claims against Local Entities because Drivers’ allegations were either too conclusory or too speculative to show, as to each Defendant or each access, that Law Enforcement Does’ purposes for obtaining the personal information were impermissible. Drivers now appeal the district courts’ dismissals of their DPPA claims, challenging the district courts’ rulings on each of these issues.

⁴Although this fact is not alleged in Potocnik’s complaint, several parties state in their briefs that Potocnik was once employed as a Minneapolis police officer.

II. Statute of Limitations

Because the DPPA does not contain its own statute of limitations, the parties agree that Drivers' claims are subject to the catch-all, four-year statute of limitations in 28 U.S.C. § 1658(a). Under § 1658(a), except as otherwise provided by law, "a civil action arising under an Act of Congress enacted after [December 1, 1990,] may not be commenced later than 4 years after the cause of action accrues." Subsection (b) of the provision states that, "[n]otwithstanding subsection (a)," securities fraud claims may be brought no later than the earlier of "2 years after the discovery of the facts constituting the violation" or "5 years after such violation." 28 U.S.C. § 1658(b). Congress added this subsection as part of the Sarbanes-Oxley Act of 2002. Pub. L. No. 107-204, § 804(a), 116 Stat. 745, 801.

Since the parties dispute only the meaning of § 1658, whether the statute of limitations bars Drivers' claims is a question of law that we review *de novo*. Smithrud v. City of St. Paul, 746 F.3d 391, 395 (8th Cir. 2014). Drivers argue that the discovery rule applies and that therefore their causes of action accrued when they discovered, or with due diligence should have discovered, that the alleged violations occurred—*i.e.*, when they received their audits from DPS. Defendants argue that we should apply the occurrence rule and hold that Drivers' causes of action accrued when the allegedly impermissible accesses occurred. The occurrence rule thus would bar claims based on accesses that occurred more than four years prior to the filing of the complaints.

Traditionally, in federal-question cases, we have applied the discovery rule as the default statute-of-limitations rule in the absence of a contrary directive from Congress. *E.g.*, Comcast of Ill. X v. Multi-Vision Elecs., Inc., 491 F.3d 938, 944 (8th Cir. 2007) (citing Union Pac. R.R. Co. v. Beckham, 138 F.3d 325, 330 (8th Cir. 1998)). Other federal courts also have generally taken this approach. *See Connors v. Hallmark & Son Coal Co.*, 935 F.2d 336, 342 (D.C. Cir. 1991) (noting that "the

discovery rule is the general accrual rule in federal courts” and listing cases); see also Rotella v. Wood, 528 U.S. 549, 555 (2000) (noting that lower “[f]ederal courts . . . generally apply a discovery accrual rule when a statute is silent on the issue”).

As the Supreme Court has explicitly pointed out, however, it has never adopted that position as its own, TRW Inc. v. Andrews, 534 U.S. 19, 27 (2001), and several Supreme Court opinions cast doubt on our application of the discovery rule as the default rule. In TRW, the Court addressed the question when liability “arises” for purposes of the statute of limitations in the Fair Credit Reporting Act (FCRA). Like the DPPA, the FCRA limits the disclosure of certain information about individuals—specifically, information in an individual’s credit report—unless it is for statutorily enumerated purposes. Id. at 23 (citing 15 U.S.C. §§ 1681b, 1681e(a)-(b)). The Court considered the purposes of the FCRA and concluded that the “FCRA does not govern an area of the law that cries out for application of a discovery rule.” Id. at 28. Although the Court did not expressly disavow federal courts’ application of a discovery rule in the face of congressional silence, it made clear that the text and structure of a statute can “evince Congress’ intent to preclude judicial implication of a discovery rule.” Id. at 27-28. At the time, the FCRA’s statute of limitations generally required that an action be brought “within two years from the date on which the liability arises” but created an exception for willful misrepresentations, in which case the action must have been commenced “within two years after discovery by the individual of the misrepresentation.” 15 U.S.C. § 1681p (1994) (amended 2003). Noting that it defied common sense to transform the discovery-rule exception into the general rule and that such a construction would almost always render the discovery-rule exception superfluous, the Court held that the discovery rule did not govern the FCRA’s general statute of limitations. TRW, 534 U.S. at 23, 28-29.

A recent Supreme Court decision offers additional guidance on how the appropriate statute of limitations is to be determined. In Gabelli v. SEC, the Court considered whether, in an enforcement action by the Securities and Exchange

Commission (SEC), the five-year statute of limitations applicable to the Investment Advisers Act “begins to tick when the fraud is complete or when the fraud is discovered.” 133 S. Ct. 1216, 1219 (2013). Like 28 U.S.C. § 1658(a), the relevant provision setting forth the statute of limitations applied to various provisions throughout the U.S. Code and used language similar to that in § 1658, requiring actions to be commenced “within five years from the date when the claim first accrued.” Id. at 1220 (quoting 28 U.S.C. § 2462). The purpose of the provision was to provide a statute of limitations for actions for civil fines, penalties, or forfeiture. Id. To determine the appropriate trigger for the statute of limitations, the Court considered whether there were “textual, historical, or equitable reasons to graft a discovery rule” onto the statute of limitations. Id. at 1224. The Court stated that the most natural reading of the statute was that a claim “accrued” when the allegedly fraudulent conduct occurred, because “the standard rule is that a claim accrues when the plaintiff has a complete and present cause of action.” Id. at 1220-21 (quoting Wallace v. Kato, 549 U.S. 384, 388 (2007)) (internal quotation marks omitted). The Court focused on the policy considerations underlying all limitations provisions, explaining that “[s]tatutes of limitations are intended to ‘promote justice by preventing surprises through the revival of claims that have been allowed to slumber until evidence has been lost, memories have faded, and witnesses have disappeared.’” Id. at 1221 (quoting Order of R.R. Telegraphers v. Ry. Express Agency, Inc., 321 U.S. 342, 348-49 (1944)). The Court noted that the discovery rule “arose in 18th-century fraud cases as an ‘exception’ to the standard rule,” and noted that the “fraud discovery rule” applies when “the injury is self-concealing.” Id. at 1221-22. Nevertheless, the Court determined that a government enforcement action for securities fraud did not require application of the discovery rule in light of the government’s investigative resources and the punitive nature of civil penalties.

This appeal requires us to consider the effect of Gabelli on our precedent, as set forth in Comcast, that establishes the discovery rule as the default rule in the absence of a contrary directive from Congress. Comcast does not constrain us,

because, “[a]lthough one panel of this court ordinarily cannot overrule another panel, this rule does not apply when the earlier panel decision is cast into doubt by a decision of the Supreme Court.” Patterson v. Tenet Healthcare, Inc., 113 F.3d 832, 838 (8th Cir. 1997). More problematic is the fact that after Gabelli, we reiterated our view that the discovery rule is the default rule in Maverick Transportation, LLC v. U.S. Department of Labor, Administrative Review Board, 739 F.3d 1149, 1154 (8th Cir. 2014), in which we held that the discovery rule governed the statute of limitations under the Surface Transportation Assistance Act. Nevertheless, Maverick does not control here for two reasons. First, Maverick focused on TRW, see id., and did not discuss the effect of, or even cite, Gabelli.⁵ “[W]hen an issue is not squarely addressed in prior case law, we are not bound by precedent through *stare decisis*.” Passmore v. Astrue, 533 F.3d 658, 660 (8th Cir. 2008) (citing Brecht v. Abrahamson, 507 U.S. 619, 630-31 (1993)). Second, in Maverick, we were required to defer to the Department of Labor’s interpretation that the discovery rule applied and thus were bound to apply the agency’s version of the discovery rule as long as it was a permissible construction of the statute. 739 F.3d at 1154 (citing Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837, 842-43 (1984)).

Drivers argue that the holding in Gabelli was limited to the factual context of that case—government enforcement actions—and that the language in Gabelli characterizing the occurrence rule as the standard rule is insufficient to overrule our long-established case law. But “[f]ederal courts . . . are not ‘free to limit Supreme Court opinions precisely to the facts of each case.’ Instead, federal courts ‘are bound by the Supreme Court’s considered dicta almost as firmly as by the Court’s outright holdings’” City of Timber Lake v. Cheyenne River Sioux Tribe, 10 F.3d 554,

⁵Nor did the parties in Maverick bring Gabelli to the panel’s attention in their filings. See Webster v. Fall, 266 U.S. 507, 511 (1925) (“Questions which merely lurk in the record, neither brought to the attention of the court nor ruled upon, are not to be considered as having been so decided as to constitute precedents.”).

557 (8th Cir. 1993) (citation omitted) (quoting McCoy v. Mass. Inst. of Tech., 950 F.2d 13, 19 (1st Cir. 1991)).

We need not decide whether Gabelli completely overrules our precedent that makes the discovery rule the default rule when Congress is silent. Gabelli certainly does not “bar application of the discovery rule where precedent, structure and policy all favor such a rule.” Psihoyos v. John Wiley & Sons, Inc., 748 F.3d 120, 124 n.5 (2d Cir. 2014). But Gabelli and TRW, read together, instruct us that when the text, structure, and purpose of a limitations provision suggest that Congress may not have intended for the discovery rule to apply, courts should take into account the general policy underlying statutes of limitation, as well as equitable considerations relevant to the cause of action at hand, when determining whether to apply the discovery or occurrence rule.

Turning to the text of § 1658, to “accrue” is “[t]o come into existence as an enforceable claim or right; to arise.” Black’s Law Dictionary 21 (7th ed. 1999). TRW suggests that this definition is ambiguous, see 534 U.S. at 32 (“On balance, we conclude, the phrase ‘liability arises’ is not particularly instructive, much less dispositive of this case.”), whereas Gabelli suggests that the most natural reading is that a claim “accrues” when the alleged violation occurs, because “the standard rule is that a claim accrues when the plaintiff has a complete and present cause of action,” 133 S. Ct. at 1220-21 (quoting Wallace, 549 U.S. at 388) (internal quotation marks omitted). Drivers seek liquidated damages for each violation in the amount of \$2500, which “could presumably be awarded at the moment of [Defendants’] alleged wrongdoing, even if ‘actual damages’ did not accrue at that time.” TRW, 534 U.S. at 35. Thus, Drivers’ causes of action arguably came “into existence as an enforceable claim or right” at the time of the alleged accesses. On the other hand, to illustrate the meaning of the word “accrue,” Black’s Law Dictionary uses the example of a claim that “accrues” upon discovery of the injury. See Black’s Law Dictionary 21 (7th ed. 1999) (“[T]he plaintiff’s cause of action for silicosis did not accrue until

the plaintiff knew or had reason to know of the disease.”). Read together, the definition and the example could support the notion that the word “accrue” simply refers to the date on which the statute of limitations begins to run. See Dring v. McDonnell Douglas Corp., 58 F.3d 1323, 1327 (8th Cir. 1995) (noting that the date on which the statute of limitations begins to run “is referred to as the accrual date”). The meaning of the word “accrue” is thus not free of ambiguity.

We therefore turn to the structure of § 1658. Defendants argue that § 1658 is analogous to the statute of limitations in TRW. Like the FCRA limitations provision in TRW, § 1658 prescribes a general statute of limitations, then creates a special standard that includes an express discovery rule. Unlike the provision in TRW, however, the special standard in § 1658 that applies to securities-fraud claims includes an express occurrence rule as well. In this case, then, the principle of statutory interpretation that would prevent the exception in § 1658(b) from becoming the general rule in § 1658(a) would apply equally to both the discovery and occurrence rules.

What § 1658(b)’s structure does demonstrate, however, is that at the time Congress amended § 1658 to add subsection (b), it knew how to write statutory text that differentiated between the discovery and occurrence rules and yet chose to preserve as the general rule the more ambiguous language of § 1658(a) stating that the statute of limitations begins to run when the “cause of action accrues.” Congress’s decision to retain the word “accrues” in § 1658(a), instead of specifying the applicable rule as it did in § 1658(b), is significant. Notably, § 1658 is a catch-all statute of limitations that applies to a variety of civil actions arising under acts of Congress. Here, the text, structure, and purpose of § 1658, coupled with the ambiguous definition of “accrue,” suggest that Congress may have intended the trigger for the date of accrual to vary depending upon the specific cause of action at hand.

In these circumstances, and in light of recent Supreme Court jurisprudence, we must look to equitable and policy considerations to determine the appropriate trigger for the statute of limitations for a DPPA claim. The parties and amicus curiae, the Electronic Privacy Information Center, emphasize competing policy concerns. Drivers argue that they had no reason to know that their personal information was being impermissibly accessed. But even if Drivers had no reason to know of the alleged accesses, unlike violations grounded in fraud, latent disease, or medical malpractice, DPPA violations are not by their nature self-concealing. See TRW, 534 U.S. at 27 (noting that it is cases involving concealment or latent injuries in which the Court has recognized a prevailing discovery rule and in which “the cry for [such a] rule is loudest” (alteration in original) (quoting Rotella, 528 U.S. at 555)). The Electronic Privacy Information Center raises legitimate concerns about the ability of identity thieves to utilize sensitive personal information found in motor vehicle records and the difficulty in detecting such a crime within the applicable limitations period. But these arguments are ultimately unavailing. The FCRA also provides remedies to combat the harms of identity theft, see 15 U.S.C. §§ 1681c-1 to 1681c-2, yet even though the plaintiff in TRW was herself the victim of identity theft, the Court concluded that the occurrence rule applied, see 534 U.S. at 23-27. If the FCRA, a statute designed to protect against misuse of individuals’ sensitive, personal information, “does not govern an area of the law that cries out for application of a discovery rule,” id. at 28, then neither does the DPPA. Furthermore, faded memories and time-lost evidence pertaining to the disclosure, obtainment, or use of data are the types of considerations that statutes of limitation are intended to address. See Gabelli, 133 S. Ct. at 1221 (citing R.R. Telegraphers, 321 U.S. at 348-49).

In light of the foregoing policy considerations, as well as the text and structure of § 1658, we conclude that the statute of limitations for these DPPA violations began to run when the violations occurred. We thus affirm the dismissal of claims of violations that occurred more than four years prior to the filing of the complaints.

III. Liability of Local Entities and Law Enforcement Does

Several Local Entities argue that Drivers fail to state claims against them because Law Enforcement Does merely viewed Drivers' information and never used or "obtain[ed]" it within the meaning of § 2724. They also urge us to hold that Drivers have failed to state a claim for relief that satisfies the pleading standard as set forth in Bell Atlantic Corp. v. Twombly, 550 U.S. 544 (2007), and Ashcroft v. Iqbal, 556 U.S. 662 (2009). Drivers argue that accessing and reading data is "obtain[ment]" under the DPPA and that the district courts misapplied Twombly and Iqbal's pleading standard. We address each argument in turn.

A. The Meaning of "Obtain"

Section 2724 of the DPPA provides a cause of action for impermissible "obtain[ment], disclos[ure] or use[]" of personal information. Several Local Entities argue that the alleged accesses of information at issue do not constitute "obtain[ments]" under § 2724 of the DPPA. They contend that "obtain" means "to hold onto or possess," that there must be deprivation or physical possession of the information, and that mere viewing is not sufficient. Although the etymology of the word "obtain" shows that its derivation is a Latin word meaning "to hold on to, possess," in modern usage, "obtain" means "to gain or attain," Merriam-Webster's Collegiate Dictionary 803 (10th ed. 1998), or "to get, acquire," Bryan A. Garner, Garner's Modern American Usage 74 (3d ed. 2009). Because the personal information at issue is intangible in nature, it is gained or acquired when it is accessed or observed. Congress could not have intended to require physical procurement of intangible information. In the context of the DPPA, the word "obtain" unambiguously includes access and observation of the data.⁶

⁶Because the meaning of "obtain" in this context is unambiguous, Local Entities' various arguments that depend on interpreting ambiguity in their favor fail.

B. “Use” of the Personal Information

Several Local Entities argue that they cannot be liable under the DPPA because even if Law Enforcement Does “obtain[ed]” Drivers’ personal information, the information was never used. In support of this argument, Local Entities point to Cook v. ACS State & Local Solutions, Inc., 663 F.3d 989, 994 (8th Cir. 2011), in which we stated that “the DPPA is concerned with the ultimate use of drivers’ personal information, not how that information is obtained.” This argument plucks our statement from Cook and leaves behind the context. Cook involved the question whether a company violates the DPPA if it obtains personal information in bulk for future use or resale to third parties. Id. at 991. We held that because the intended future use of the information was for a legitimate purpose permitted under the DPPA, the fact that much of the information obtained was not “used” immediately, or at all, did not render the bulk obtainment unlawful. Id. at 994, 997. Defendants argue that this holding indicates that the DPPA is violated only when information is actually used for an improper purpose. But in fact, Cook stands for the contrary proposition. Under Cook, the fact that personal information is never put to use does not retroactively alter the purpose for which it was obtained. By the same logic, the fact that Law Enforcement Does never “used” Drivers’ personal information would not change the fact that the information was obtained for a purpose not permitted under the DPPA, in violation of § 2724. Furthermore, to read § 2724 as requiring use of the information, as some Defendants suggest, would render the word “obtains” superfluous because the provision separately prohibits impermissible “use[.]” It is clear that under § 2724, obtaining Drivers’ information without a permissible

Their contention that qualified immunity applies to Law Enforcement Does’ conduct because the meaning of “obtain” is unclear also fails for the same reason. Cf. Collier v. Dickinson, 477 F.3d 1306, 1312 (11th Cir. 2007) (“The words of the DPPA alone are ‘specific enough to establish clearly the law applicable to particular conduct and circumstances and to overcome qualified immunity.’” (quoting Vinyard v. Wilson, 311 F.3d 1340, 1350 (11th Cir. 2002))).

purpose, regardless of whether that information is subsequently used, violates the DPPA.

C. Rule 8(a)'s Pleading Standard

Local Entities argue, and the district courts held, that Drivers have fallen short of pleading a plausible claim for relief. To establish a DPPA violation, Drivers must prove that the Defendants 1) knowingly 2) obtained, disclosed, or used personal information, 3) from a motor vehicle record, 4) for a purpose not permitted. See 18 U.S.C. § 2724(a). The only issue the parties dispute is whether Drivers have sufficiently pleaded the impermissible-purpose element of their DPPA claims. The parties' arguments on this issue apply equally to the claims against Law Enforcement Does.

We review the grants of the motions to dismiss *de novo*. Richter v. Advance Auto Parts, Inc., 686 F.3d 847, 850 (8th Cir. 2012) (per curiam). When evaluating a motion to dismiss, we accept as true all factual allegations in the complaint and draw all reasonable inferences in favor of the nonmoving party, *id.*, but we are not bound to accept as true “[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements,” Iqbal, 556 U.S. at 678, or legal conclusions couched as factual allegations, Papasan v. Allain, 478 U.S. 265, 286 (1986). Under Federal Rule of Civil Procedure 8(a)(2), a complaint must contain a “short and plain statement of the claim showing that the pleader is entitled to relief.” “To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” Iqbal, 556 U.S. at 678 (quoting Twombly, 550 U.S. at 570). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.*

“Determining whether a complaint states a plausible claim for relief will . . . be a context-specific task that requires the reviewing court to draw on its judicial

experience and common sense.” Id. at 679. “Asking for plausible grounds . . . does not impose a probability requirement at the pleading stage; it simply calls for enough fact to raise a reasonable expectation that discovery will reveal evidence of” the violation. Twombly, 550 U.S. at 556. There is no requirement for direct evidence; the factual allegations may be circumstantial and “need only be enough to nudge the claim ‘across the line from conceivable to plausible.’” Cardigan Mountain Sch. v. N.H. Ins. Co., 787 F.3d 82, 88 (1st Cir. 2015) (quoting Twombly, 550 U.S. at 556).

Courts considering a motion to dismiss may choose to begin by identifying allegations that are no more than conclusions and therefore are not entitled to the assumption of truth. Iqbal, 556 U.S. at at 679. Courts may then review the remaining allegations to determine whether they are sufficient “to raise a right to relief above the speculative level, on the assumption that all the [factual] allegations in the complaint are true (even if doubtful in fact).” Twombly, 550 U.S. at 555 (citations and footnote omitted). Courts should consider whether there are lawful, “obvious alternative explanation[s]” for the alleged conduct, because “[w]here a complaint pleads facts that are merely consistent with a defendant’s liability, it stops short of the line between possibility and plausibility of entitlement to relief.” Iqbal, 556 U.S. at 678, 682 (quoting Twombly, 550 U.S. at 557, 567 (brackets omitted)) (internal quotation marks omitted). If the alternative explanations are not sufficiently convincing, however, the complaint states a plausible claim for relief, because “[f]erret[ing] out the most likely reason for the defendants’ actions is not appropriate at the pleadings stage.” Watson Carpet & Floor Covering, Inc. v. Mohawk Indus., Inc., 648 F.3d 452, 458 (6th Cir. 2011).

Drivers allege that Law Enforcement Does obtained their information “for a purpose not permitted under the DPPA” and that none of Law Enforcement Does’ activities “fell within the DPPA’s permitted exceptions for procurement of [Drivers’] private information.” Because these allegations simply recite the impermissible-purpose element of a DPPA cause of action, they should be disregarded in

determining whether the complaint states a claim for relief. See Iqbal, 556 U.S. at 678. The question, then, is whether Drivers’ remaining, nonconclusory allegations state a plausible claim that Drivers’ personal information was obtained for an impermissible purpose. The district courts held that Drivers’ complaints did not plead facts with sufficient specificity to raise a right to relief above the speculative level. According to the district courts, they could not draw the inference that any particular Law Enforcement Doe’s access was for an impermissible purpose without resorting to speculation based solely on the collective allegations and the sheer volume of accesses.

Each Defendant’s alleged conduct must be assessed independently to ensure that Drivers have pleaded sufficient facts regarding that Defendant’s impermissible purpose to state a facially plausible claim to relief against that Defendant. Cf. id. at 682-83 (refusing to infer discriminatory state of mind of one government actor based on allegedly discriminatory acts by others); Wilson v. Northcutt, 441 F.3d 586, 591 (8th Cir. 2006) (“Liability for damages for a federal constitutional tort is personal, so each defendant’s conduct must be independently assessed.”). But assessing the allegations against each Defendant independently is not the same as assessing them in isolation. “[T]he complaint should be read as a whole, not parsed piece by piece to determine whether each allegation, in isolation, is plausible.” Braden v. Wal-Mart Stores, Inc., 588 F.3d 585, 594 (8th Cir. 2009). Furthermore, allegations concerning data accesses that do not themselves constitute violations because they are barred by the statute of limitations still may be considered in assessing the plausibility of timely claims. See Nat’l R.R. Passenger Corp. v. Morgan, 536 U.S. 101, 113 (2002) (stating that plaintiff may use pre-limitations-period acts as background evidence in support of a timely claim); U.S. EPA v. City of Green Forest, 921 F.2d 1394, 1409 (8th Cir. 1990) (“[T]here is no rule that automatically excludes evidence pre-dating a statute of limitations period.”).

Viewing, for example, each of Bass's and Mitchell's complaints as a whole, there is no lawful, obvious alternative explanation for why a Driver would have the personal information in her motor vehicle record accessed hundreds of times by dozens of government entities throughout the state of Minnesota in the span of a few years when she alleges she has committed no crimes, has not to her knowledge been involved in any criminal investigation, and has reason to believe Law Enforcement Does may have a personal interest in her. It is reasonable to infer that many of the accesses were not within the scope of official government functions. Such reasoning may carry a claim against a particular Defendant to the brink of plausibility. Nevertheless, when merely consistent with the liability of any particular Defendant, these generalized allegations, standing alone, "stop[] short of the line between possibility and plausibility of entitlement to relief." Twombly, 550 U.S. at 557 (original brackets and internal quotations omitted). When there are no allegations of concerted activity, something more is needed to nudge the allegations across the line of plausibility and tie the conduct of specific Defendants to a more general inference of impermissible purpose.

We therefore turn to the allegations that relate to particular Local Entities. Although most of the Drivers allege that they had professional relationships with law enforcement personnel, or a degree of local fame, Drivers have not pleaded, for example, that they had a relationship with particular officers or agents of Local Entities, that the alleged accesses occurred shortly after interactions with officers or agents of Local Entities, or that certain Law Enforcement Does' accesses were timed in such a way that they corresponded with a significant event that could explain the interest in Drivers' personal information. Instead, the only facts pleaded in the complaints that are specific to particular Defendants are the number of accesses through each agency's station and the times and dates of each access. Although insufficient to plead a plausible claim for relief against every Defendant, these allegations do reveal suspicious access patterns and timing of accesses that nudge

claims against some Defendants “across the line from conceivable to plausible.” Twombly, 550 U.S. at 570.

For example, a suspicious access pattern occurs when Law Enforcement Does access a Driver’s information on the same day or within the span of a few hours through multiple, unrelated agencies. Common sense suggests it would be unusual for multiple, unrelated law enforcement or other government agencies—often based in different parts of Minnesota—to obtain a Driver’s personal information within minutes or hours of each other or even on the same day. And although there may be occasions where there are permissible purposes to justify these accesses—such as when agencies work together in an investigation or in preparation for an event—these are not obvious alternative explanations that render an inference of impermissible purpose merely speculative or implausible.

In addition, Drivers allege numerous accesses between the hours of 11 p.m. and 6 a.m. (late-night accesses). Common sense suggests that during late-night or early-morning hours, law enforcement staff and other government employees may be subject to less supervision and more likely to look up Drivers’ personal information out of boredom, curiosity, or romantic interest. Although a single late-night access may not raise a red flag, and allegations of late-night accesses alone might well be insufficient to state a plausible claim for relief, the multiple late-night accesses, when viewed in combination with the other allegations, raise some Drivers’ claims against certain Defendants to the level of plausibility.⁷

⁷Several Local Entities suggest that Drivers have waived any argument that the suspicious access patterns and timing of accesses render their claims for relief plausible because Drivers failed to raise this argument below. Drivers’ argument, however, is plainly embraced by their complaints and fairly encompassed by their arguments made below that the volume, dates, and times of the accesses were inconsistent with any proper government purpose. On appeal, Drivers merely recite facts already laid out in the complaint in a manner that helps to establish their

The district court in Bass, McDonough, and Potocnik declined to infer that Law Enforcement Does had an impermissible purpose for the obtainments in part because of the “presumption of regularity,” under which, “in the absence of clear evidence to the contrary,” courts presume that public officers “have properly discharged their official duties.” United States v. Armstrong, 517 U.S. 456, 464 (1996) (quoting United States v. Chem. Found., Inc., 272 U.S. 1, 14-15 (1926)). Whatever weight the “presumption of regularity” might otherwise have at this stage in the litigation, Drivers have sufficiently rebutted it by alleging high volumes and suspicious timing of accesses and by pointing to the legislative auditor’s report finding that at least half of Minnesota law enforcement officers were misusing personal information in the database. See Bracy v. Gramley, 520 U.S. 899, 909 (1997) (refusing to apply the presumption of regularity when it was “soundly rebutted”).

The district court in Mitchell expressed concern that allowing these types of claims to surmount the plausibility hurdle would leave courts with “no coherent and workable way to distinguish between DPPA claims that should survive a motion to dismiss and those that should not.” Ensuring that only plausible claims that meet the Iqbal and Twombly pleading standard survive a motion to dismiss in these cases necessarily involves a certain degree of line drawing. But such line drawing is inevitable, since courts must assess the plausibility of plaintiffs’ grounds for relief by drawing on their own “judicial experience and common sense.” Iqbal, 556 U.S. at 679; see also Adam N. Steinman, The Pleading Problem, 62 Stan. L. Rev. 1293, 1345 (2010) (“Ultimately, the line-drawing challenge is unavoidable. As long as we agree that a complaint cannot just allege that ‘defendant violated plaintiff’s rights in a way that entitles plaintiff to relief,’ courts will need to police what is and is not an adequate identification of the events underlying a plaintiff’s claim.”). In the unique

connectivity. Cf. Topchian v. JPMorgan Chase Bank, N.A., 760 F.3d 843, 849 (8th Cir. 2014) (considering a plaintiff’s fleshed-out arguments on appeal because “it is the facts alleged in a complaint, and not the legal theories, that state a claim”).

context of these cases, determining which accesses support a plausible claim for relief may well be a time-consuming process.

We therefore turn to each Driver's complaint and assess the allegations against each Defendant.

1. Bass's Complaint

Bass alleges that she served as a negotiator and attorney for Law Enforcement Labor Services, Minnesota's largest law enforcement union, beginning in 2005 and ending in 2011. Since March 2005, her personal information was viewed via name search more than 750 times by approximately 340 government personnel. She alleges that she does not have a criminal record and has committed no crimes that could justify the accesses. She claims not only that various law enforcement personnel accessed her data without a permissible purpose, but also that individuals in the Anoka, Hennepin, and Stearns County Attorney offices accessed her data in preparation for hearings or court proceedings that were adverse to her clients.

Bass's audit shows frequent late-night accesses. For example, during the period within the statute of limitations, 61 of the 278 accesses occurred between the hours of 11:00 p.m. and 6:00 a.m. The audit also reveals numerous suspicious access patterns. For example, on January 8, 2007, there were 19 accesses of Bass's personal information at various times throughout the day through stations from nine different agencies from around the state. The next day, there were 25 accesses throughout the day through seven different agencies from around the state. The day after that, there were 20 accesses throughout the day through eight different agencies throughout the state. Suspicious access patterns continued during the period within the statute of limitations. For example, on May 5, 2009, there were four accesses of Bass's

personal information by the Wayzata PD⁸ between 7:08 and 7:09 a.m., an access by the Two Harbors PD at 7:38 a.m., two accesses by the St. Anthony PD at 9:16 a.m., and two accesses by the Minneapolis PD at 11:47 a.m.

There are 69 agencies⁹ with alleged violations during the limitations period. Of those, 38 agencies¹⁰ did not have a history of frequent suspicious accesses before the limitations period and did not, during the limitations period, engage in multiple

⁸Hereinafter we abbreviate “police department” to “PD.”

⁹These include the Alexandria PD, Anoka County Attorney, Anoka County Sheriff, Anoka Courts, Anoka PD, Appleton PD, Bemidji PD, Benton County Sheriff, Big Lake PD, Blaine PD, Bloomington PD, Brooklyn Center PD, Burnsville PD, Champlin PD, Clay County Sheriff, Crow Wing County Sheriff, Dakota County Sheriff, Dayton PD, Dodge County Sheriff, Eagan PD, Elk River PD, Fairmont PD, Faribault PD, Farmington PD, Fridley PD, Gaylord PD, Hennepin County Attorney, Hennepin County Sheriff, Houston County Sheriff, Jackson PD, Jordan PD, Kandiyohi County Sheriff, Kasson PD, Maple Grove PD, Marshall PD, Minneapolis PD, Minnetonka PD, Minnetrista PD, Moorhead PD, Mounds View PD, New Hope PD, North St. Paul PD, Oakdale PD, Osseo PD, Pipestone County Sheriff, Plymouth PD, Prior Lake PD, Ramsey County Dispatch Center, Rice County Sheriff, Richfield PD, Robbinsdale PD, Roseville PD, Sartell PD, Scott County Sheriff, Shakopee PD, Sherburne County Sheriff, Sleepy Eye PD, St. Anthony PD, St. Cloud PD, St. Francis PD, St. Louis Park PD, Stearns County Attorney, Stearns County Sheriff, Stillwater PD, Two Harbors PD, Washington County Sheriff, Wayzata PD, Winona PD, and Wright County Sheriff.

¹⁰These include the Alexandria PD, Anoka County Attorney, Anoka Courts, Anoka PD, Appleton PD, Blaine PD, Bloomington PD, Burnsville PD, Clay County Sheriff, Crow Wing County Sheriff, Dakota County Sheriff, Dayton PD, Dodge County Sheriff, Eagan PD, Fairmont PD, Faribault PD, Farmington PD, Fridley PD, Hennepin County Attorney, Hennepin County Sheriff, Jackson PD, Jordan PD, Kandiyohi County Sheriff, Minnetonka PD, Minnetrista PD, North St. Paul PD, Plymouth PD, Prior Lake PD, Rice County Sheriff, Richfield PD, Robbinsdale PD, Roseville PD, Sartell PD, Scott County Sheriff, Sleepy Eye PD, St. Louis Park PD, Stearns County Attorney, and Winona PD.

late-night accesses or participate in any suspicious access patterns. To infer that the particular Defendants allegedly responsible for these non-suspicious accesses had impermissible purposes would require sheer conjecture rooted solely in the blanket allegations of misconduct, Bass's professional interactions with law enforcement personnel in general, and the high volume of collective accesses. Bass's allegations against the Local Entities and Law Enforcement Does responsible for accesses through those agencies' stations thus fail to state a claim for relief.

Information accesses by Law Enforcement Does through the remaining 31 agencies¹¹ fall into one of three categories: 1) accesses on the same day as or within a few hours of accesses by other, unrelated entities during the limitations period; 2) multiple late-night accesses during the limitations period; or 3) a history of frequent suspicious accesses fitting the above criteria, even if prior to the limitations period, coupled with accesses within the limitations period. Local Entities have not offered an "obvious alternative explanation" that renders these accesses non-suspicious. Local Entities argue, for example, that officers may have been looking up Bass's information to verify her identity prior to meetings with Bass. This explanation generally would not justify the accesses, since a police officer's union activities are not within his or her official government duties. Nor is this explanation obviously consistent with multiple close-in-time look-ups through unrelated agencies. The other law enforcement tasks that Local Entities proffer for the look-ups—such as approval of gun permits; computer forensics investigations; and verification of the

¹¹These include the Anoka County Sheriff, Bemidji PD, Benton County Sheriff, Big Lake PD, Brooklyn Center PD, Champlin PD, Elk River PD, Gaylord PD, Houston County Sheriff, Kasson PD, Maple Grove PD, Marshall PD, Minneapolis PD, Moorhead PD, Mounds View PD, New Hope PD, Oakdale PD, Osseo PD, Pipestone County Sheriff, Ramsey County Dispatch Center, Shakopee PD, Sherburne County Sheriff, St. Anthony PD, St. Cloud PD, St. Francis PD, Stearns County Sheriff, Stillwater PD, Two Harbors PD, Washington County Sheriff, Wayzata PD, and Wright County Sheriff.

identity of witnesses, victims, or drivers after a license-plate check—may be plausible, but they are not sufficiently convincing to undermine the reasonable inference of impermissible purpose that arises from the multiple late-night look-ups and suspicious access patterns reflected in the audit.

Local Entities also note that law enforcement personnel frequently work late-night shifts and perform online investigative work throughout the night. But if we accept, as we must, Bass’s allegation that she committed no crimes, she was unlikely to be the subject of any investigation by law enforcement, much less numerous law enforcement agencies from across the state. The possibility that discovery will reveal that Bass was, in fact, the subject of a state-wide investigation, or separate investigations by dozens of different agencies, is not sufficiently convincing an explanation to render her claims implausible.

Thus, allegations against all Law Enforcement Does responsible for any accesses within the limitations window through the remaining 31 agencies’ stations state facially plausible claims for relief. Although not all of the accesses during the limitations period through these agencies’ stations occurred during late-night or early-morning hours or as part of a suspicious access pattern, the fact that any suspicious accesses occurred through these agencies render suspect the other accesses through their stations. Law Enforcement Does at these agencies may have lacked sufficient training to deter misuse. Furthermore, the various accesses may have been performed by the same person, or that person may have prompted his or her coworkers to query Bass’s information. Bass’s allegations related to all of the accesses within the limitations period through these remaining 31 agencies state plausible claims for relief, and so we reverse the dismissal of the timely claims against Law Enforcement

Does responsible for these accesses. The dismissal of her claims against all other Law Enforcement Does is affirmed.¹²

Local Entities have offered no additional arguments for why they are not liable for individual Law Enforcement Does' accesses through their agencies' stations. We therefore reverse the dismissal of the timely claims against the following Local Entities: Anoka County, City of Bemidji, Benton County, City of Big Lake, City of Brooklyn Center, City of Champlin, City of Elk River, City of Gaylord, Houston County, City of Kasson, City of Maple Grove, City of Marshall, City of Minneapolis, City of Moorhead, City of Mounds View, City of New Hope, City of Oakdale, City of Osseo, Pipestone County, Ramsey County, City of Shakopee, Sherburne County, City of St. Anthony, City of St. Cloud, City of St. Francis, Stearns County, City of Stillwater, City of Two Harbors, Washington County, City of Wayzata, and Wright County. The dismissal of Bass's claims against all other Local Entities is affirmed.

2. McDonough's Complaint

McDonough alleges that in 2005 she became a crime reporter for the television station Fox 9 in the Twin Cities and is now an investigator and reporter for local station KSTP. Her work as a reporter has involved contact with numerous law enforcement personnel. Between 2006 and 2013, her information was accessed nearly 500 times by more than 170 government personnel from about 70 different agencies or departments. Although McDonough does not allege that she committed no crimes—and, according to the parties, has had two driving-while-impaired (DWI) incidents—several of McDonough's interactions with police suggest that law enforcement officers had acquired an unusual interest in her. In 2007 or 2008, DPS

¹²The district court may determine that it is more feasible to postpone dismissal until the substitution of named defendants. We simply wish to make clear that Bass has not stated claims against these individuals.

Commissioner Dohman, who was the Maple Grove Chief of Police at the time, told McDonough, “[P]eople are fascinated by you. Be a little careful.” In 2011, McDonough overheard a police officer whom she did not know tell another officer that she was an “out-of-stater” and lived in Minnetonka. And in 2012, as McDonough was walking through City Hall in Minneapolis, a police officer with whom she was unfamiliar told her he liked her new car. Because these allegations reflect a pattern of personal interest in McDonough on the part of law enforcement officers, they add to the plausibility of McDonough’s allegations of impermissible purpose.

McDonough’s audit also shows frequent late-night accesses and suspicious access patterns. For example, 58 of the 471 accesses of McDonough’s personal information listed in her audit occurred between the hours of 11:00 p.m. and 6:00 a.m. And during the week of November 2, 2008, through November 8, 2008, McDonough’s personal information was accessed 178 times through 46 different governmental agencies’ or business entities’ stations. Although Defendant Hennepin County asserts, and McDonough does not dispute, that this was around the same time that she was charged with DWI, that fact does not obviously explain why individuals from so many different agencies—including, for example, 21 different local police departments from various parts of the state and the Twin Cities metro area—would have a permissible purpose to look up her personal information. Suspicious access patterns and late-night accesses also occurred on several occasions during the limitations period. For the same reasons outlined above in the analysis of Bass’s complaint, these allegations nudge McDonough’s claims against certain Defendants across the line from conceivable to plausible.

Local Entities argue that there are a number of alternative explanations that could justify the obtainments of McDonough’s information. They argue, for example, that Law Enforcement Does may have accessed McDonough’s information in order to use her photo for photo lineups. It is not obvious, however, that it is a regular

practice for Minnesota law enforcement to use name searches in the database to composite photos for a photo lineup. Nor is it obvious that law enforcement personnel would utilize the photo of a well-known reporter for an anonymous photo lineup. Without the benefit of discovery related to law enforcement practices and the use and functions of the DPS system, we cannot say that this is a convincing or obvious alternative explanation for the accesses. Local Entities also argue that the accesses could have involved responding to calls of trespassing reporters. It is not obvious that McDonough, an experienced reporter, frequently trespassed in the middle of the night or in different parts of Minnesota throughout a single day. Finally, Local Entities argue that officers may have needed to verify McDonough's identity while she was covering stories or to ensure security at events such as the 2008 Republican National Convention. At this stage, we are not convinced that dozens of law enforcement agencies would have needed to verify McDonough's identity for events such as the 2008 Republican National Convention. Many of the suspicious accesses—and all of the accesses within the limitations period—occurred after the Convention. Moreover, it is not obvious that law enforcement officers regularly use the database to verify the identity of reporters like McDonough whenever the reporter is covering a story nearby. And even if that is a regular practice, it is an even less convincing explanation for late-night or multiple same-day look-ups.

We therefore turn to analyzing the alleged accesses. There are 15 agencies¹³ with alleged violations within the limitations period. Seven of these agencies¹⁴ did

¹³These include the Carver County Sheriff, Golden Valley Deputy Registrar, Hancock PD, Hennepin County Sheriff, Hennepin Courts, Minneapolis PD, Minnetonka PD, Ramsey County Sheriff, Rice County Sheriff, South St. Paul Deputy Registrar, St. Paul Deputy Registrar, State Patrol, Three Rivers Park District PD, West Metro Plymouth Exam Station, and Wright County Sheriff.

¹⁴These include the Golden Valley Deputy Registrar, Hennepin Courts, Rice County Sheriff, South St. Paul Deputy Registrar, St. Paul Deputy Registrar, Three

not have a history of frequent suspicious accesses, and Law Enforcement Does did not, during the limitations period, engage in multiple late-night accesses or participate in any suspicious access patterns through these agencies. The allegations regarding obtainments through these agencies thus fail to state a claim for relief. The audit reflects that Law Enforcement Does through the remaining eight agencies¹⁵ accessed McDonough's personal information on the same day as or within a few hours of accesses by other, unrelated entities during the limitations period; performed multiple late-night accesses during the limitations period; or had a history of frequent suspicious accesses prior to the limitations period, coupled with one or more accesses during the limitations period. Allegations against the Law Enforcement Does responsible for accesses within the limitations window through these eight agencies' stations thus state facially plausible claims for relief, and we reverse the dismissal of the timely claims against them. We also reverse the dismissal of the timely claims against the following Local Entities allegedly liable for those accesses: Carver County, City of Hancock, Hennepin County, City of Minneapolis, City of Minnetonka, Ramsey County, and Wright County. The dismissal of McDonough's claims against all other Local Entities and Law Enforcement Does is affirmed.

3. Mitchell's Complaint

Mitchell alleges that in 2004, she became a news anchor and sports reporter for Fox 9 News and presently works for Fox 9, co-anchors Fox at Five, and is an anchor and reporter for Fox 9 Sports. She has also served as a sideline reporter for the NFL on Fox broadcasts. During her career, she has met and interviewed numerous law enforcement personnel. She alleges that she has not committed any crimes that would

Rivers Park District PD, and West Metro Plymouth Exam Station.

¹⁵These include the Carver County Sheriff, Hancock PD, Hennepin County Sheriff, Minneapolis PD, Minnetonka PD, Ramsey County Sheriff, State Patrol, and Wright County Sheriff.

authorize the accesses of her personal information and that the information was obtained without any probable cause or reasonable suspicion to believe she had engaged in any criminal activity or any activity even remotely related to criminal activity. In January 2013, the Department of Natural Resources notified Mitchell that her information had been accessed by an individual for an impermissible purpose. She subsequently requested an audit, which revealed that her information had been accessed approximately 219 times by approximately 50 entities between 2005 and 2013. All of these allegations carry Mitchell's assertions of impermissible purpose to the brink of plausibility.

As in the cases of McDonough and Bass, Mitchell's audit reveals several suspicious access patterns. For example, within the span of an hour on November 25, 2007, her information was accessed through the stations of three different agencies based in different parts of Minnesota: at 3:36 p.m. through the Ramsey County Sheriff's station, then at 4:08 and 4:10 p.m. through the Blue Earth PD, and then at 4:23 p.m. through the Rice County Sheriff's office. In addition, Mitchell's audit shows frequent late-night or early-morning accesses, with 37 of the 219 accesses of her personal information listed in the audit occurring between the hours of 11:00 p.m. and 6:00 a.m.

In support of their argument that Mitchell has not asserted plausible allegations of impermissible purpose, Local Entities note that there are other Dawn Mitchells in Minnesota, some of whom have criminal records, and point to a Hennepin County Attorney's affidavit and attached public records. But at the motion-to-dismiss stage, we must draw all reasonable inferences in favor of Mitchell, and without the benefit of discovery, including discovery related to the use and functions of the database, we cannot say that this alternative explanation is so obvious as to render Mitchell's claim

of impermissible purpose facially implausible.¹⁶ Other than the argument based on the multiple Dawn Mitchells, Local Entities offer essentially the same “alternative explanations” that were offered for the accesses of McDonough’s and Bass’s information. For the same reasons, these “alternative explanations” are not sufficiently obvious, or do not sufficiently account for the late-night accesses and the close-in-time accesses by different agencies, to render Mitchell’s claims against certain Local Entities inadequately pleaded.

Turning to an analysis of the alleged obtainments, there are 15 agencies¹⁷ with accesses within the limitations period. Only four of those agencies¹⁸ have multiple late-night accesses within the limitations period; accesses within the limitations period on the same day or within a few hours of accesses through other, unrelated agencies; or a history of frequent suspicious accesses prior to the limitations period. Mitchell’s allegations relating to the timing and patterns of accesses at those four agencies thus nudge her claims against the allegedly responsible Law Enforcement Does and Local Entities across the line of plausibility. We therefore reverse the dismissal of Mitchell’s timely claims against the Law Enforcement Does responsible for accesses through those four agencies. We also reverse the dismissal of Mitchell’s timely claims against the Cities of Minneapolis and Edina, since they are the only two entity defendants to which those agencies’ accesses can be attributed. The dismissal

¹⁶It is not obvious, for example, that the database is, or was in the past, set up in such a way that officers would never be able to tell, until accessing any or all of Mitchell’s personal information, that she was the wrong Dawn Mitchell.

¹⁷These include the Anoka County Sheriff; Blaine PD; Chaska Driver’s License Office; Department of Corrections; Edina Driver’s License Office; Edina PD; Freeborn County Court Services; Hennepin Courts; Hopkins PD; Maple Grove PD; Minneapolis PD; St. Croix County, Wisconsin, 911; St. Louis Park Driver’s License Office; St. Paul PD; and State Patrol.

¹⁸These include the Edina PD; Minneapolis PD; St. Croix County, Wisconsin, 911; and State Patrol.

of Mitchell's claims against all other Local Entities and Law Enforcement Does is affirmed.

4. Potocnik's Complaint

Potocnik alleges that since 2003, more than 200 law enforcement personnel from approximately 40 different departments or agencies have accessed his information approximately 420 times. The audit attached to Potocnik's complaint reveals that 308 of the 416 listed accesses—and 47 of the 50 accesses within the limitations period—were performed through the Minneapolis PD's station.

There are only four agencies with accesses within the limitations period: the Minneapolis PD, Gilbert PD, Dilworth PD, and St. Louis County Sheriff's office. Of these, the Dilworth PD had only one early-morning access and no other accesses whatsoever. Although numerous users in the Minneapolis PD frequently accessed Potocnik's information, the City of Minneapolis is not a party to this appeal. Potocnik has pursued a separate action against Minneapolis and the Law Enforcement Does responsible for accesses through the Minneapolis PD. See Potocnik v. City of Minneapolis, No. 14-1215(DSD/TNL), 2014 WL 4829454 (D. Minn. Sept. 29, 2014).

The St. Louis County Sheriff's office and Gilbert PD each accessed Potocnik's information only once during the limitations period, but they did have a history of suspicious accesses. Nevertheless, Potocnik has pleaded no underlying facts that explain why he would garner Law Enforcement Does' interest. Although the parties have indicated that Potocnik is a former police officer who was once under investigation, there are no allegations in the complaint of any relationship he may have had with any law enforcement agency, professional or otherwise. Nor are there any allegations that would explain why law enforcement officers would have an unusually high level of interest in Potocnik. Potocnik alleges in conclusory fashion

that his personal information was obtained “without probable cause or reasonable suspicion.” Potocnik does not allege that he committed no crimes that would justify the accesses. Potocnik asks us to infer from the sheer volume of accesses, the large majority of which are attributable to the Minneapolis PD, and from a few past suspicious accesses through the Gilbert PD and St. Louis County Sheriff stations, that the accesses were for an impermissible purpose. His allegations of underlying facts lack the specificity necessary to give rise to a reasonable inference that the remaining Defendants obtained his personal information for an impermissible purpose. We therefore affirm the dismissal of Potocnik’s complaint against all Law Enforcement Does and Local Entities. We express no opinion about Potocnik’s claims in the separate action.

IV. Commissioners and DPS Does

Drivers¹⁹ challenge the district court’s dismissal of the claims against Commissioners. The district court held that the DPPA did not create a private right of action for Commissioners’ alleged negligence in mismanaging information from motor vehicle records and that Commissioners could be held liable only if the complaint established that “the Commissioners *themselves*” had an impermissible purpose for disclosing Drivers’ personal information to Law Enforcement Does. On appeal, Commissioners contend that the allegations against them fail to state a claim either because they did not have the necessary mental state required to violate the Act or because they have qualified immunity. The parties’ arguments on this issue apply equally to DPS Does.

¹⁹Throughout this section, “Drivers” refers only to Bass, McDonough, and Potocnik, the three Drivers who brought claims against Commissioners and DPS Does.

Although the district court did not address the issue of qualified immunity, we review grants of motions to dismiss *de novo* and may affirm on any grounds that the record supports, including qualified immunity. See Christiansen v. W. Branch Cmty. Sch. Dist., 674 F.3d 927, 933-34 (8th Cir. 2012). “Qualified immunity gives government officials breathing room to make reasonable but mistaken judgments about open legal questions.” Ashcroft v. al-Kidd, 131 S. Ct. 2074, 2085 (2011). “[G]overnment officials performing discretionary functions generally are shielded from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known.” Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982). A government official “violates clearly established law when, at the time of the challenged conduct, ‘[t]he contours of [a] right [are] sufficiently clear’ that every ‘reasonable official would have understood that what he is doing violates that right.’” al-Kidd, 131 S. Ct. at 2084 (alterations in original).

The DPPA’s provisions limiting the disclosure, obtainment, or use of personal information from a motor vehicle record include a mental state requirement. Section 2724 provides: “A person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court.” Commissioners argue that they cannot be held liable to Drivers under § 2724 because the required mental state, “knowingly,” applies not only to the “disclos[ure]” of the information, but also to the phrase, “for a purpose not permitted.” In essence, Commissioners contend that DMV employees can be held liable only if they had actual knowledge of Law Enforcement Does’ impermissible purposes for obtaining the information. Commissioners also suggest that they are liable only if they themselves harbored an impermissible “purpose” for the disclosure. Drivers argue that the word “knowingly” in § 2724 modifies only the phrase denoting the act—“obtains, discloses or uses”—and not the

phrase “for a purpose not permitted.” Drivers contend that, at the very least, Commissioners had an obligation under the DPPA to make some effort to ascertain each Law Enforcement Doe’s purpose prior to each disclosure.

Several circuits have weighed in on the scope of the DPPA’s mental state requirement. Although none have squarely addressed the issue before us, their opinions could support either of the parties’ conflicting interpretations. Compare Gordon v. Softech Int’l, Inc., 726 F.3d 42, 53-54 (2d Cir. 2013) (holding, in the context of resellers, that the DPPA implicitly imposes a duty to exercise reasonable care in responding to requests for personal information), Pichler v. UNITE, 542 F.3d 380, 396 n.21 (3d Cir. 2008) (primarily addressing an ignorance-of-the-law defense but noting agreement with the district court that the word “knowingly” modifies only the act requirement), and Senne v. Village of Palatine, 695 F.3d 597, 603 (7th Cir. 2012) (en banc) (same, stating that “[v]oluntary action . . . is sufficient to satisfy the mens rea element of the DPPA”), with Roth v. Guzman, 650 F.3d 603, 611-12 (6th Cir. 2011) (holding that state employees who disclosed information to an obtainer who explicitly stated a permissible purpose were entitled to qualified immunity because the focus should be on the use for which the information was disclosed, not the undisclosed use for which it was obtained).

The circuits’ varied interpretations of § 2724’s mental state element reflect a lack of clarity regarding 1) to which element or elements the “know[ledge]” requirement applies; 2) the standard of care, if any, that disclosers must exercise when ascertaining the purpose for an information request; and 3) whether the word “purpose” in § 2724 refers to the discloser’s purpose for divulging the information or the obtainer’s purpose for requesting it. Even if, at the time of the disclosures in the instant action, it was clearly established that a discloser has a duty under the DPPA to make some effort to ascertain a recipient’s purpose, it was not clearly established that the ascertained purpose must be express and explicit. Drivers allege

that DPS issued passwords to police officers, employees at sheriffs' offices, court staff, or other similarly situated government agents in connection with their jobs. There are no allegations that DPS issued passwords to agents or officers whose job duties did not require the use of personal information in motor vehicle records and who nevertheless accessed Drivers' personal information. Drivers allege that Law Enforcement Does received training about proper use of the database and that the website used to log on to the database stated, "Access to this service is for authorized personnel only conducting official business" Law Enforcement Does thus implicitly certified a permissible purpose each time they logged on. In these circumstances, we cannot say that, at the time of the alleged accesses, any reasonable official would have understood that DPS's policy of allowing the above-described government employees password-protected access to the database violated Drivers' rights under the DPPA.

Drivers also allege that Commissioners and DPS Does knew of the widespread misuse of the system and "knowingly disclosed" Drivers' personal information by "failing to safeguard and monitor the database" and by "willfully refusing to correct the misuses." These allegations, at most, allege negligence or recklessness. Even assuming that the DPPA imposes a duty of some degree of care on DPS officials, that duty of care was not clearly established at the time of the alleged violations. To the extent that Drivers attempt to allege, without support, that Commissioners and DPS Does actually knew that the particular disclosures alleged in the complaint were for impermissible purposes, such bald allegations are conclusory and are properly disregarded when determining whether the complaint survives a motion to dismiss. See Iqbal, 556 U.S. at 681, 683. We therefore affirm the dismissal of Bass's, McDonough's, and Potocnik's claims against the Commissioners and DPS Does.²⁰

²⁰Although qualified immunity does not necessarily prevent an award of equitable relief against government officials in their official capacities, e.g., Grantham v. Trickey, 21 F.3d 289, 295-96 (8th Cir. 1994), Drivers have not argued that their prospective-relief claims should be analyzed differently than their claims

V. Conclusion

As set forth above, the dismissals of Bass's, McDonough's, and Mitchell's claims are affirmed in part and reversed in part, and the cases are remanded for further proceedings consistent with this opinion. The dismissal of Potocnik's claims is affirmed.

for damages and explicitly stated in their filings below that they were not pleading any official capacity claims. Bass and McDonough also stated in their complaint captions that they were asserting claims against the Commissioners in their individual capacity.