RECOMMENDED FOR FULL-TEXT PUBLICATION
Pursuant to Sixth Circuit Rule 206

File Name: 11a0155p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

ERIC T. ROTH, individually and on behalf of all others similarly situated; MARY BETH ROTH, individually and on behalf of all others similarly situated; ERIN C. KENNY, individually and on behalf of all others similarly situated,

Plaintiffs-Appellees,

v.

HENRY GUZMAN, Director, Ohio Department of Public Safety; MIKE RANKIN, Registrar, Ohio Bureau of Motor Vehicles,

Defendants-Appellants.

No. 10-3542

Appeal from the United States District Court
for the Southern District of Ohio at Cincinnati.
No. 09-00253—Michael R. Barrett, District Judge.

Argued: April 26, 2011

Decided and Filed: June 13, 2011

Before: GUY, CLAY, and McKEAGUE, Circuit Judges.

COUNSEL

ARGUED: Elisabeth A. Long, OHIO ATTORNEY GENERAL'S OFFICE, Columbus, Ohio, for Appellants. Charles T. Lester, Jr., ERIC C. DETERS & ASSOCIATES, Independence, Kentucky, for Appellees. **ON BRIEF:** Elisabeth A. Long, Benjamin C. Mizer, OHIO ATTORNEY GENERAL'S OFFICE, Columbus, Ohio, for Appellants. Charles T. Lester, Jr., ERIC C. DETERS & ASSOCIATES, Independence, Kentucky, for Appellees.

GUY, J., delivered the opinion of the court, in which McKEAGUE, J., joined. CLAY, J. (pp. 21–26), delivered a separate dissenting opinion.

OPINION

RALPH B. GUY, JR., Circuit Judge. Defendants Henry Guzman, Director of the Ohio Department of Public Safety, and Mike Rankin, Registrar of the Ohio Bureau of Motor Vehicles, appeal from the district court's determination that they were not entitled to qualified immunity from suit in this putative class action alleging violation of the plaintiffs' rights under the federal Driver's Privacy Protection Act (DPPA), 18 U.S.C. §§ 2721-2725, and 42 U.S.C. § 1983. Without challenging other aspects of the decision denying their motion to dismiss, defendants argue that their alleged conduct did not violate the plaintiffs' clearly established federal rights as delineated by the DPPA. We agree, and for the reasons that follow, we reverse.

I.

This court has jurisdiction over the defendants' interlocutory appeal from the denial of qualified immunity, but only to the extent that the appeal turns on issues of law. *Mitchell v. Forsyth*, 472 U.S. 511, 530 (1985); *Estate of Carter v. City of Detroit*, 408 F.3d 305, 309-10 (6th Cir. 2005). We review the denial of qualified immunity *de novo*, and the same standard applies to the motion for judgment on the pleadings under Fed. R. Civ. P. 12(c) as to a motion to dismiss under Fed. R. Civ. P. 12(b)(6). *Williams v. Mehra*, 186 F.3d 685, 689-90 (6th Cir. 1999) (en banc); *EEOC v. J.H. Routh Packing Co.*, 246 F.3d 850, 851 (6th Cir. 2001). To survive a motion to dismiss, the complaint must "contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009); (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).[1]

[1] Apart from the issue of qualified immunity, the district court also found that plaintiffs had standing; that Eleventh Amendment immunity did not bar the claims for money damages; and that statutory rights under the DPPA are enforceable both directly and under § 1983. None of these issues are before us.

A. Driver's Privacy Protection Act of 1994

The federal DPPA was enacted in response to growing concerns over the ease with which stalkers and other criminals could obtain personal information from state departments of motor vehicles.[2] *Reno v. Condon*, 528 U.S. 141, 143-44 (2000). Congress was also concerned about the practice in many states of selling personal information from motor vehicle records to businesses, marketers, and others for, at times, significant revenue. *Id.* The DPPA, held to be a proper exercise of the power to regulate interstate commerce, established a regulatory scheme that both mandates and restricts the disclosure of personal information from records maintained by state motor vehicle departments. *Id*. at 148.

At all times relevant to this case, the DPPA, as amended, imposed the following general prohibitions against the disclosure of personal information obtained from an individual's motor vehicle record:

> (a) **In general.**–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*:
>
> > (1) *personal information*, as defined in 18 U.S.C. [§] 2725(3), *about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section*; or
> >
> > (2) *highly restricted personal information*, as defined in 18 U.S.C. § 2725(4), about any individual obtained by the department in connection with a motor vehicle record, *without the express consent of the person to whom such information applies, except uses permitted in subsections (b)(1), (b)(4), (b)(6), and (b)(9)*; *Provided*, That subsection (a)(2) shall not in any way affect the use of organ donation information on an individual's driver's license or affect the administration of organ donation initiatives in the States.

[2] Among several well-publicized cases was the 1989 murder of the actress Rebecca Shaeffer by a stalker who obtained her unlisted address from information that she had provided to the California DMV.

18 U.S.C. § 2721(a)(1)-(2) (emphasis added). "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*. at § 2725(3). "Highly restricted personal information" is defined as "an individual's photograph or image, social security number, medical or disability information." *Id*. at § 2725(4).

Section 2721(b) carves out both mandatory and permissive exceptions to the general prohibitions in subsection (a). *Id.* at § 2721(b). First, states *must* disclose personal information for use in carrying out the purposes of several federal statutes not relevant here. Second, states *may* disclose personal information (subject to § 2721(a)(2)), for any of the permissible uses or purposes listed in § 2721(b)(1)-(14). Eleven of these permissible uses—including for "use in the normal course of business" under § 2721(b)(3)—authorize nonconsensual disclosure of personal information. *Id.* at § 2721(b)(1)-(10) and (14). The other three permissible uses require the express consent of the persons to whom the information pertains. *Id*. at § 2721(b)(11)-(13).

The DPPA also regulates the "resale or redisclosure" of personal information in § 2721(c), which provides, in pertinent part, that: "An *authorized recipient* of personal information (except a recipient under subsection (b)(11) or (12)) may resell or redisclose the information *only for a use permitted under subsection (b)* (but not for uses under subsection (b)(11) or (b)(12))." *Id*. at § 2721(c) (emphasis added). Subsection (c) also imposes a record-keeping obligation on "[a]ny authorized recipient (except a recipient under subsection (b)(11)) that resells or rediscloses personal information covered by this chapter" to keep for five years "records identifying each person or entity that receives information and the permitted purpose for which the information will be used and must make such records available to the motor vehicle department upon request." *Id*.[3]

[3]Disclosure under subsections (b)(11) (for any use) and (b)(12) (for bulk distributions for surveys, marketing or solicitation) is permissible "if the State has obtained the express consent of the person to whom such personal information pertains." *Id.* at § 2721(b)(11)-(12) (as amended eff. June 1, 2000).

The DPPA makes it unlawful for "any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under [§] 2721(b)," or "to make false representation to obtain any personal information from an individual's motor vehicle record." 18 U.S.C. § 2722(a)-(b). A person who knowingly violates the DPPA is subject to criminal fine, *id*. at § 2723(a), and may be held civilly liable for actual damages (but not less than $2,500 in liquidated damages), punitive damages, attorney fees, and appropriate equitable relief, *id*. at § 2724. A "person" is defined as an individual, organization or entity, "but does not include a State or agency thereof," *id*. at § 2725(2). Instead, the Attorney General may impose civil penalties if a state has a policy or practice of "substantial noncompliance" with the DPPA, *id*. at § 2723(b) (civil penalty of not more than $5,000 per day).

B. Factual Allegations

Plaintiffs Eric Roth, Mary Beth Roth, and Erin Kenny brought this action on behalf of themselves and other similarly situated drivers licensed in Ohio any time after April 8, 2004, whose "personal information" as defined by the DPPA was disclosed, sold, or otherwise disseminated by the individual defendants while acting as agents or employees of the Ohio Department of Public Safety (DPS) and/or the Ohio Bureau of Motor Vehicles (BMV). Specifically, plaintiffs alleged that Shadowsoft, Inc., a Texas corporation specializing in "public records database distribution," unlawfully acquired a large database from the DPS and/or BMV that contained "personal information" belonging to "hundreds of thousands" of drivers licensed in Ohio. Defendants admitted in their Answer that the BMV disclosed personal information to Shadowsoft in response to its requests for public records for a purportedly permissible purpose under the DPPA—namely, for use in the "normal course of business" under 18 U.S.C. § 2721(b)(3)—and attached documents associated with Shadowsoft's requests to their Answer.[4]

[4]Defendants' Answer alleged that Guzman did not become director of the DPS until February 9, 2007, and that Rankin did not become Registrar of the BMV until April 16, 2007. Defendants argue that, if the case were to go forward, they could not be held personally liable for disclosures that occurred before they took office.

Plaintiffs further alleged, upon information and belief, that Shadowsoft "transferred the database *in totum*" to The Source for Public Data, LP, (PublicData), which, in turn, allegedly made the personal information "available for search and sale on its website, www.publicdata.com." There is no claim that the defendants disclosed information directly to PublicData, only a general allegation that plaintiffs' personal information was disseminated without obtaining their express consent and not for a purpose otherwise permitted by the DPPA. Defendants, for their part, generally denied having unlawfully disclosed, sold, or otherwise disseminated personal information to Shadowsoft, PublicData, or any other entity.

More specifically, the documents attached to defendants' Answer, and therefore properly considered as part of the pleading for all purposes, shed light on the challenged disclosures. *See* FED. R. CIV. P. 10(c) ("A copy of a written instrument that is an exhibit to a pleading is a part of the pleading for all purposes."); *Commercial Money Ctr., Inc. v. Ill. Union Ins. Co.*, 508 F.3d 327, 335 (6th Cir. 2007). First, in Exhibit A, defendants attached two Record Requests made by an individual on behalf of Shadowsoft using Ohio's BMV Form 1173. The first request sought driver's license information on a monthly basis, and the second requested vehicle registration records. On each form, the requester indicated, by way of a check mark, that the requests were being made for a permissible purpose corresponding to the "normal course of business" exception under § 2721(b)(3). Form 1173 also informed the requester of the restrictions placed on the resale or redisclosure of the information consistent with the DPPA's limitations found in § 2721(c). The requester provided her name, the company name, an address, and telephone numbers, but left blank the spaces that requested other identifying information (*e.g.*, social security number, driver's license number, tax identification number, vendor number or professional license number).[5]

[5]Form 1173 references Ohio's parallel statute governing disclosures of personal information from motor vehicle records rather than the provisions of the DPPA. There is no dispute that the Ohio statute mirrors the DPPA, except that defendants maintain that the Ohio law directs that disclosures must be made whenever permissible under the DPPA.

Defendants' Exhibit B to the Answer, titled "Agreement for the Sale of Information (to be used with BMV Form 1173)," was executed in December 2004 by Shadowsoft and the comptroller of the BMV. That Agreement provided, among other things, that Shadowsoft would receive copies of public records on a monthly basis and would pay the associated fees on a monthly basis. Also, Shadowsoft warranted that it and all its personnel were familiar with the Ohio Driver Privacy Protection Act, and agreed that all users would abide by both federal and state laws restricting access to personal information from motor vehicle records and governing the resale or redisclosure of such information. In addition, Shadowsoft agreed not to provide information obtained under the Agreement to any other person without entering into an agreement that included these prohibitions.

Accepting the factual allegations as true, we assume that the BMV made "bulk" disclosures of personal information from motor vehicle records to Shadowsoft for what was asserted to be a permissible purpose, and that Shadowsoft resold or redisclosed the information "in bulk" to PublicData. While defendants do not deny that PublicData resold or redisclosed the information in violation of the DPPA, there are also no facts alleged regarding the operation of PublicData or the disclosures allegedly made by it.[6]

C. Procedural History

Plaintiffs commenced this action in April 2009, and amended their complaint shortly thereafter. Defendants moved for judgment on the pleadings, seeking dismissal of the amended complaint on a number of grounds. That motion was fully briefed, argued, and supplemented. In an order entered March 31, 2010, the district court rejected each of the defendants' contentions and concluded, in pertinent part, that the defendants were not entitled to qualified immunity from suit on the plaintiffs' claims

---

[6]At one point, plaintiffs disavowed that their claims were based on how the information was allegedly misused by Shadowsoft. ("Plaintiffs have brought this suit because of an unlawful *disclosure* made by the individual Defendants, not because of how the information was ultimately misused by Shadowsoft. In other words, it makes no difference whether Shadowsoft sold the unlawfully disclosed information on the internet, or whether it used the information to tabulate how many 'Johns' or 'Jims' are driving in Ohio. The Defendants[']liability is based on the fact that they were prohibited from disclosing the information except to an 'authorized recipient[.]'")

under the DPPA or § 1983. Briefly, the district court concluded that plaintiffs had plausibly alleged that the defendants' conduct violated a statutory right by alleging that defendants had disclosed personal information for a purpose not permitted by the DPPA. Further, the district court found that this right was "clearly established" by the plain language of the statute and that, in light of the incomplete information provided in the Record Requests, a reasonable official would have understood that the disclosures would violate the DPPA. Defendants appealed, and the district court entered a stay pending appeal.

II.

Qualified immunity protects government officials and employees performing discretionary functions "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); *see also Saucier v. Katz*, 533 U.S. 194, 202 (2001). In deciding claims of qualified immunity, we must determine: (1) whether the facts alleged or shown by the plaintiffs make out a violation of federal statutory or constitutional right; and (2) whether that right was "clearly established" at the time of the defendants' alleged misconduct. *Pearson v. Callahan*, 129 S. Ct. 808, 815-16 (2009). Although it is "often appropriate" to resolve these questions sequentially, it is no longer mandatory that the court do so. *Id*. at 818; *see also Waeschle v. Dragovic*, 576 F.3d 539, 543-44 (6th Cir. 2009). For a right to be "clearly established," the "contours of the right must be sufficiently clear that a reasonable official would understand that what he is doing violates that right." *Anderson v. Creighton*, 483 U.S. 635, 640 (1987). Once raised as a defense, plaintiffs bear the burden of demonstrating that the defendants are not entitled to qualified immunity. *Silberstein v. City of Dayton*, 440 F.3d 306, 311 (6th Cir. 2006).

A. Purportedly Permissible Use

Plaintiffs argue that, as the district court found, defendants violated the DPPA by disclosing personal information for a use not permitted under § 2721(b). In reaching

this conclusion, the district court interpreted the DPPA's provisions as imposing liability, presumably criminal as well as civil, whether or not the state official knew that the disclosure was not actually for a proper purpose. Defendants argue (1) that this is a misreading of the DPPA that would require the state to verify a requester's true intentions; and (2) that, even if a correct interpretation, it was not a clearly established right of which a reasonable person would have known.

1. Violation

The pleadings establish that the disclosures in this case were purportedly made under § 2721(b)(3), which permits nonconsented disclosure of personal information (but not highly restricted personal information):

> (3) For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only—
>
> > (A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and
> >
> > (B) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.

18 U.S.C. § 2721(b)(3). As outlined above, the disclosures made by the Ohio BMV were made based on Shadowsoft's express written representations that the disclosures were "for use in the normal course of business"—as permitted by § 2721(b)(3) (and Ohio law)—although plaintiffs allege that Shadowsoft falsely represented this to be the purpose of the disclosures.

The finding that this alleged a violation of the DPPA rested on the district court's interpretation of § 2724(a), which provides that: "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[.]" The district court relied on *Pichler v. UNITE*, 228 F.R.D. 230, 241-42 (E.D.

Pa. 2005), *aff'd on other grounds*, 542 F.3d 380 (3d Cir. 2008), which reasoned that the location of the adverb "knowingly" in this provision suggested an intention to limit the reach of the knowledge requirement. That is, the court in *Pichler* found that "knowingly" modifies only the first part—the two clauses defining the act element—and not the last part—the third clause defining the purpose element. Without agreeing or disagreeing with *Pichler*, we find that it does not address the question presented in this case.

In *Pichler*, the labor union defendants recorded license plate numbers from cars in an employee parking lot and obtained the employees' addresses from motor vehicle records through Westlaw and a private investigator's requests to the state motor vehicle department. The court in *Pichler* rejected the defendants' claim that they could not be liable because they did not know that the requester's purpose in *obtaining* the personal information was not permissible, explaining:

> If one could not violate the DPPA without "knowing[]" that the purpose for which he "obtain[ed]," "disclose[d]" or "use[d]" motor vehicle information was unlawful, then every defendant would get at least one free bite at the violation-of-privacy apple. After all, anyone could claim that he did not "know" his purpose to be impermissible until a court interpreted the DPPA to proscribe that purpose. Even after such a ruling, a defendant could manufacture a slightly different purpose for his conduct and then claim ignorance of whether the DPPA prohibited the new purpose. A plaintiff could recover only if the defendant repeatedly violated her privacy and lacked sufficient creativity to conjure up some conceivable purpose that no court had yet considered.

Id. at 242; *see also Rios v. Direct Mail Express, Inc.*, 435 F. Supp. 2d 1199, 1204-05 (S.D. Fla. 2006) (relying on *Pichler* to conclude that plaintiffs were not required to prove that a direct marketer who knowingly obtained records from the Florida DMV also knew that Florida had not obtained the express consent required under the amended DPPA to release the records to a mass marketer under (b)(12)).

It is one thing to say that a defendant's ignorance that his own conduct violates the law is not a defense, but it is another, we think, to conclude that a defendant is liable for a knowing disclosure made for a permissible purpose any time the purpose was

misrepresented or the information was later misused or improperly redisclosed by the requester or any other entity. Here, the pleadings establish that the defendants' act, the knowing disclosure of personal information, was *for an explicitly permissible purpose*. Moreover, the plaintiffs complain that Shadowsoft falsely represented its intended use and redisclosed the information to PublicData, which made the information available for search and sale to its customers for unspecified purposes.

If no distinction is made between the use for which the *defendants disclosed* the information, and the undisclosed use for which it was obtained, subsequently misused or impermissibly redisclosed by the recipient, the DPPA becomes essentially a strict liability statute. Every subsequent misuse could be traced back to a violation by the state official. Rather than place all of the liability with the state officials, however, the DPPA makes it unlawful for any person (excluding the states and their agencies) to knowingly obtain, disclose, or use the information for a purpose not permitted by the DPPA. While it may be that this and other courts will find that one's ignorance of the law is no defense to a claim under the DPPA, this was not the defendants' claim in this case. Rather, defendants' alleged that *their* disclosures were for a permitted purpose, even if Shadowsoft's undisclosed intention was to obtain the personal information for a purpose not permitted by the DPPA.

That the defendants' disclosure was expressly for a permitted purpose distinguishes this case from *Welch v. Theodorides-Bustle*, 677 F. Supp. 2d 1283 (N.D. Fla. 2010). Similar to this case, state officials were alleged to have violated the DPPA by making disclosures of personal information in bulk to Shadowsoft, which, in turn, redisclosed the information to PublicData. The defendants did not deny that from PublicData's website, "an internet user can access the information for any or no reason—or on a whim." *Id*. at 1286. Unlike this case, however, the court in *Welch* specifically found that the contracts entered into with Shadowsoft did not specify either a proper purpose for the disclosures, or the uses and further disclosures it would or would not make. No claim could be made in that case that disclosures were for a purportedly permissible purpose, and the court rejected the suggestion that the

defendants could rely on § 2721(b)(1) (for use by a government agency in carrying out its functions). Not surprisingly, the court also found that the state officials' disclosures for *an unspecified purpose,* when the DPPA requires that personal information not be disclosed *except* as provided for in § 2721(b), violated clearly established federal law of which the defendants' should have known. *Id*. (citing *Collier v. Dickenson*, 477 F.3d 1306 (11th Cir. 2007).

2. Clearly Established

Even if we accept that the DPPA may be read to impose liability on a state official in his individual capacity when personal information disclosed for a purportedly permissible purpose was actually obtained for an impermissible purpose, we cannot agree that this right was clearly established at the time of the disclosures (putting aside the allegation that the disclosures were only made under the defendants' authority for a short time).

The district court acknowledged that there was (and is) no binding precedent from the Supreme Court, the Sixth Circuit, the district court itself, or other circuits deciding the issues raised in this case such as would render the asserted right "clearly established." *See Risbridger v. Connelly*, 275 F.3d 565, 569 (6th Cir. 2002). "'This is not to say that an official action is protected by qualified immunity unless the very action in question has previously been held unlawful, but it is to say that in the light of pre-existing law the unlawfulness must be apparent.'" *Wilson v. Layne*, 526 U.S. 603, 615 (1999) (quoting *Anderson*, 483 U.S. at 641). An official may be on notice that his conduct violates established law even in novel factual circumstances. *See Hope v. Pelzer*, 536 U.S. 730, 741 (2002).

Relying on the Eleventh Circuit decision in *Collier* affirming the denial of qualified immunity to state officials for disclosures under the DPPA, the district court concluded that the plain language of the DPPA clearly established an individual's right to be free from disclosures for purposes not permitted under § 2721(b). As is clear from a closer reading of *Collier*, however, the district court did not engage in a sufficiently particularized reading of the rights that are clearly established by the DPPA.

In *Collier*, the plaintiffs alleged that the state officials in Florida violated the DPPA by releasing personal information from driver's license records to a mass marketer without first obtaining the driver's express consent. The court in *Collier* found not only that the DPPA, as amended, required express consent for bulk distribution of surveys, marketing or solicitations in § 2721(b)(12), but also that the Supreme Court's decision in *Condon* specifically recognized (1) that following the amendments in 2000, states could no longer infer consent from a driver's failure to "opt-out" of disclosures, and (2) that states were bound by the mandates of the DPPA irrespective of any conflicting state law. *Collier*, 477 F.3d at 1312. The same cannot be said for the alleged violation in this case based on the defendants' failure to discover Shadowsoft's true intentions.[7]

Finally, the district court rejected defendants' contention that this interpretation made the state BMV an insurer rather than simply a gatekeeper that may rely on the requester's declaration that the disclosure would be for a permitted purpose. The district court explained as follows:

> While Defendants may be properly characterized as gatekeepers, this does not mean that they may forfeit this role entirely and adopt without question the representations of entities such as Shadowsoft who make requests for personal information. The Court finds the following discussion applicable, even though it is outside the context of the DPPA:
>
> > Qualified immunity is intended to allow officials to render intelligent decisions even though they may, upon further reflection, be deemed to have been erroneous. It is not intended to allow individual officers to abdicate their decision-making obligations in blind reliance on

[7] Another Eleventh Circuit decision interpreting the DPPA also arises out of the failure of the State of Florida to amend its statutes to comply with the amendments to the federal DPPA that changed the manner for obtaining consent from an "opt-out" to an "opt-in" procedure. *See Kehoe v. Fid. Fed. Bank & Trust*, 421 F.3d 1209, 1210 (11th Cir. 2005) ("Forty-nine states immediately passed legislation to ensure compliance with this amendment to the DPPA. Florida was the only state that did not immediately comply. Instead, Florida waited until May 13, 2004, to amend its public records statute to comply with the DPPA.") (holding that no actual damages were required to recover liquidated damages), *cert. denied*, 126 S. Ct. 1612 (2006). Notably, while concurring in the denial of *certiorari* in *Kehoe*, Justice Scalia, joined by Justice Alito, noted that there were two important issues in the case: (1) whether actual damages must be shown, and (2) whether the bank that purchased vehicle registration information for purposes of solicitation can be held liable if it did not know that the state had failed to comply with the "express consent" requirement. *See* 126 S. Ct. at 1612.

> state statutes. This is especially true in this instance where the officers involved, unlike police officers who frequently have little rule-making authority, are endowed with independent policy-making authority and have an obligation to make reasoned decisions with respect to programs and policies which they promulgate, regardless of whether those programs and policies are promulgated in accordance with State law.
>
> *F. Buddie Contracting, Ltd. v. Cuyahoga Community College Dist.*, 31 F. Supp. 2d 584, 589-590 (N.D. Ohio 1998) (finding that officials were not entitled to qualified immunity where there was evidence that affirmative action policy was unconstitutional even though the policy was enacted in compliance with state law).
>
> In this instance, those with policy-making authority have made no effort [to] ensure that requests for information are legitimate. Based on the allegations before the Court, Defendants take any request at face value and without any regard to the accuracy of the information. The Court notes that while the Record Request included places for Shadowsoft to provide its tax identification number, vendor number, professional license number, and license, Shadowsoft never completed this part of the form. Despite this lack of information, Defendants granted Shadowsoft's request for information. This indicates to the Court that Defendants proceeded with "blind reliance" on any request made. While Defendants place value in the Agreement between ODPS and Shadowsoft, the Court finds reliance on such an agreement at best naive. By simply visiting the PublicData website, Defendants would have discovered that just as Plaintiffs allege, the information Defendants were providing was available to anyone with a credit card.

Certainly, there is no claim by defendants that they did anything to affirmatively verify that Shadowsoft's request was for the use it stated. At the same time, nothing about the incomplete requester information would have told defendants that Shadowsoft was misrepresenting the use it intended to make of the personal information it was requesting. Nor did Shadowsoft's Record Requests give defendants a reason to visit PublicData's website. Whether or not it would have been prudent for the BMV to investigate Shadowsoft before making any disclosures, this is neither an obligation imposed by the terms of the DPPA, nor one that has been "clearly established" under the governing case law.

The suggestion that defendants are not entitled to qualified immunity because defendants could not have reasonably believed that Shadowsoft was a "legitimate business"—a term not defined by the DPPA—misses the mark. Plaintiffs did not allege or argue that Shadowsoft was, in fact, anything but a "legitimate business."[8] Indeed, the district court's focus was on what it viewed to be defendants' "blind reliance" on Shadowsoft's representations and not on a failure to verify that Shadowsoft was a "legitimate business." The logic of this argument seems to be that if defendants had verified Shadowsoft's corporate existence—as plaintiffs alleged that Shadowsoft was a Texas corporation—the defendants might have found reason to question the veracity of Shadowsoft's representation that it was requesting personal information for a permissible purpose. It is not explained, however, how a reasonable official would have known that it would violate the DPPA to make a disclosure for an expressly permissible purpose, to an entity plaintiffs do not claim to be illegitimate, because the defendants did not investigate the legitimacy of that business.

B. Bulk Disclosures under § 2721(b)(3)

Defendants recognize that plaintiffs have asserted a second basis for finding that the disclosures to Shadowsoft violated the DPPA. That is, plaintiffs contend that even if the personal information had been requested for use in the "normal course of business," "bulk" disclosures are not authorized for requests made under § 2721(b)(3). The district court did not reach this issue, however.

The parties agree that the starting point is the ordinary meaning of the statute. *Mills Music, Inc. v. Snyder*, 469 U.S. 153, 164 (1985) ("In construing a federal statute it is appropriate to assume that the ordinary meaning of the language that Congress employed 'accurately expresses the legislative purpose.'") (citation omitted). If the language of the statute is clear, the plain meaning of the text must be enforced. *United States v. Ron Pair Enters., Inc.*, 489 U.S. 235, 241 (1989). "The plainness or ambiguity of statutory language is determined by reference to the language itself, the specific

[8]Nor did plaintiffs contend that there were any material questions of fact in dispute concerning Shadowsoft's legal status at the time of the disclosure requests.

context in which that language is used, and the broader context of the statute as a whole." *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997). When a plain reading "leads to ambiguous or unreasonable results, a court may look to legislative history to interpret a statute." *Limited, Inc. v. Comm'r*, 286 F.3d 324, 332 (6th Cir. 2002).

Quoted in full above, § 2721(b)(3) provides that state officials may disclose personal information "[f]or use in the normal course of business . . . to verify the accuracy of personal information submitted by the individual to the business," and to correct inaccurate personal information for the purposes of "preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against the individual." Plaintiffs interpret the references to "the individual" in § 2721(b)(3) as unambiguously limiting disclosure to personal information pertaining to one individual at a time. Defendants counter that "individual" in this subsection does not refer to *how many* requests may be made at one time, but rather to the *basis* for disclosures permitted under this subsection. The Fifth Circuit, the only circuit to decide this issue, rejected the same arguments in *Taylor v. Acxiom Corp.*, 612 F.3d 325, 335 (5th Cir. 2010), *cert. denied*, 131 S. Ct. 908 (2011).

Texas, like at least eleven other states, allows persons or entities to purchase magnetic tapes of the database of driver's license records upon certification of a lawful purpose under the DPPA. *Id*. at 332. The defendants in *Taylor* were third parties who did not use all of the records immediately, but maintained databases to either use in the future (non-resellers) or to resell to others for lawful purposes (resellers). The plaintiffs in *Taylor* argued that maintaining records not actually used was itself an impermissible purpose; in other words, that "'buying the records in bulk with an expectation and purpose of valid potential use is not a permissible use under the DPPA." *Id*. at 334. Examining § 2721(b)(3) in the context of all fourteen permissible uses under § 2721(b), the court emphasized that only one subsection limits permissible uses to *individual* motor vehicle records, while only one other subsection limits permissible uses to *bulk* distributions. *Id*. at 335; *compare* § 2721(b)(11) ("[f]or any other use in response to requests for individual motor vehicle records if the State has obtained the express

consent of the person to whom such personal information pertains"), *with* § 2721(b)(12) ("[f]or bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains"). For the rest of the permissible uses, the court found there was more than one reasonable interpretation: "individual release, bulk release, or both." *Id.* at 335. The court explained:

> It does not make sense that Congress would expressly limit states to individual distribution with one permissible use if Congress intended to limit *all* of the permissible uses to individual distribution. If Congress intended only individual distribution, one would expect either Congress to expressly limit all uses or, at least, to remain silent on the matter. Likewise, if Congress intended only bulk distribution, it makes no sense to expressly limit one of the fourteen uses to bulk distribution and not the others. The text of the statute strongly indicates that it allows both individual and bulk distribution.

Id. at 336. We agree. Plaintiffs in this case do not offer any authority or persuasive argument for concluding that § 2721(b)(3) clearly and unambiguously limits disclosure of personal information to one individual at a time.[9]

To resolve the ambiguity, both parties point to aspects of the legislative history to support their positions but nothing speaks directly to the issue of "bulk" disclosures under § 2721(b)(3). More generally, Congress expressed an intention "to strike 'a critical balance between legitimate governmental and business needs for this information, and the fundamental right of our people to privacy and safety.'" *Russell v. Choicepoint Servs., Inc.*, 302 F. Supp. 2d 450, 456 (E.D. La. 2004) (quoting 139 Cong. Rec. S15, 763 (1993)). Although plaintiffs rely on statements from the legislative history reflecting an intention to give individuals control over the release of their personal information, those statements are again directed at the bulk sale of personal information for direct marketing purposes.

---

[9] Plaintiffs also misrepresent *Locate.Plus.Com, Inc. v. Iowa Dept. of Transp.*, 650 N.W.2d 609, 616 (Iowa 2002), as holding that the § 2721(b)(3) exception only authorizes the disclosure of information belonging to a specific individual and not the entire driving public. However, that case involved a request for disclosure by a private business for the purpose of reformatting the information for resale to law enforcement agencies, which the Court held was not among the permissible purposes of § 2721(b).

A statement by the sponsor of the DPPA in the House expressed concern first with the need to address the ease with which criminals and strangers could obtain driver's license information and second with the desire to curb the sale of DMV databases to direct marketers for commercial purposes by requiring consent. *Taylor*, 612 F.3d at 336-37 (quoting statement of Rep. Moran Feb. 4, 1994, 1994 WL 212698 (F.D.C.H.)). In that same statement, however, the sponsor also expressed the intention that common uses being made of the information at the time—including by businesses verifying personal information—should continue unfettered. *Id*. at 336.

Notably, the amendments to the DPPA, which restricted further the bulk distribution provision to require express as opposed to implied consent, did not adopt a consent requirement for disclosure under § 2721(b)(3), or clarify that requests for disclosure under § 2721(b)(3) should be for one person's records at a time. The Fifth Circuit was also persuaded by a Department of Justice (DOJ) advisory opinion issued in October 1998, concluding that the DPPA allowed the State of Massachusetts to release personal information to a commercial distributor who would disseminate the information to any other authorized recipients or entities that use the information solely for authorized purposes. *Taylor*, 612 F.3d at 339. We agree that the DOJ's advisory opinion is inconsistent with the notion that bulk distribution is prohibited by the DPPA. *Id*.

Finally, the court in *Taylor* concluded that the plaintiffs' reading of § 2721(b)(3) would lead to "essentially absurd results," explaining:

> At a checkout line at a grocery store or similar establishment, when a customer wishes to pay by (or cash) a check, and presents a driver's license as identification, it is obviously wholly impractical to require the merchant for each such customer to submit a separate individual request to the state motor vehicle department to verify the accuracy of the personal information submitted by the customer, under section 2721(b)(3). Any such process would obviously take way too long to be of any use to either the customer or the merchant, and would moreover flood the state department with more requests than it could possibly handle. So, the merchant buys the state department's entire data base and from it extracts on that occasion that particular customer's information, and later performs the same task as to the next such customer in the line.

> Plaintiffs would have us hold that the merchant violates the DPPA by acquiring the data base even though every single actual use made of it is an authorized use under section 2721(b), so long as there is at least one name in the data base as to which no actual use is made.

Id. at 337. The court then analogized the situation to the purchase of a set of legal reporters, which a lawyer purchases for the *purpose* of legal research even though the attorney would never read every opinion in each volume. *Id*.

As interpreted by the court in *Taylor*, plaintiffs could not establish a violation of the DPPA merely because the defendants sold personal information from motor vehicle records in bulk where the disclosure was for use, or potential use, in "the normal course of business" under § 2721(b)(3). The purchase in bulk for use as needed for a permitted purpose under § 2721(b)(3), described by some courts as "stockpiling," has been found not to violate the DPPA by several district courts. *See, e.g.*, *Wiles v. ASCOM Transp. Sys., Inc. (Wiles II)*, No. 3:10-cv-28-H, 2011 WL 672652 (W.D. Ky. Feb. 17, 2011) (unpublished); *Cook v. ACS State and Local Solutions, Inc.*, 756 F. Supp. 2d 1104 (W.D. Mo. 2010).

Although the district court did not decide this issue in the first instance, it is apparent to us that, as a matter of law, it was not clearly established at the time of defendants' conduct that "stockpiling" or bulk disclosures of personal information for a permissible purpose under § 2721(b)(3) would violate the DPPA. For this reason, plaintiffs cannot overcome a claim of qualified immunity on this theory.

III.

To the extent that the plaintiffs could prove a violation of the DPPA based on the allegation that Shadowsoft misrepresented itself as having a proper purpose under § 2721(b)(3) or that the disclosures were made in bulk under § 2721(b)(3), we find the contours of such rights were not sufficiently clear that a reasonable official would have understood at the time that the disclosures would violate such rights. Accordingly, we **REVERSE** the district court's denial of qualified immunity with respect to claims under

either the DPPA or § 1983, and **REMAND** for entry of judgment in favor of defendants Guzman and Rankin.

DISSENT

CLAY, Circuit Judge, dissenting. While I do not take issue with the majority's conclusion that nothing in the Drivers Privacy Protection Act ("DPPA" or the "Act"), 18 U.S.C. § 2721, *et seq.*, prohibits the bulk disclosure of personal information contained in drivers' records, I respectfully dissent from the majority's determination that the disclosure of such records to Shadowsoft by officials at the Ohio Department of Public Safety and the Ohio Bureau of Motor Vehicles (collectively, "BMV Officials"), without reasonably inquiring into whether Shadowsoft was a legitimate business using the records for a permissible purpose, was not a violation of a clearly established statutory requirement.

While, as the majority notes, we have no binding case authority to guide us in addressing the claims raised in this case, we do have the statutory language of the DPPA. Under the factual scenario and procedural posture of the case now before us, I agree with the district court that the language of the DPPA is, in itself, sufficient to defeat qualified immunity for Defendants.[1]

Defendants argue that the DPPA does not impose on them any obligation to verify how the information that they disclose will be used. Instead, if they disclose information that is used for an impermissible purpose, then "a driver may seek relief against the entity that violated the DPPA, not the State." (Defs.' Br. at 15.) Plaintiffs counter that "[t]he DPPA is clear: if the Defendants disclosed information for a purpose

[1]The district court held that "a reasonable official would have understood that a disclosure of information for a purpose other than one permitted by the DPPA would violate the DPPA." (Dist. Ct. Op. at 19-20.)

that did not meet an exception to the DPPA, then they are in violation of the Statute."[2] (Pls.' Br. at 10.)

The majority opinion circumvents the legal question of what duty the DPPA imposes on Defendants by making the finding that Defendants disclosed drivers' information to Shadowsoft "for an explicitly permissible purpose," though Shadowsoft later used the information impermissibly. (Maj. Op. at p. 11 (emphasis omitted).) In doing so, the majority reasons that as long as a requestor represents to BMV Officials that it will use drivers' personal information in accordance with a DPPA exception, BMV Officials do not violate the Act if they then knowingly disclose that information.

There are two insurmountable problems with the majority's approach. The first is simple, but dispositive—the record, on this judgment on the pleadings, is too vastly underdeveloped for the majority to make the factual findings necessary to logically support its conclusion. The evidence in the record insufficiently addresses any number of necessary questions, such as: what is Shadowsoft's legal status? What is Shadowsoft's relationship to PublicData? What did Shadowsoft represent to BMV Officials during contract negotiations? What did BMV Officials actually know about Shadowsoft at the time of disclosure? Did Shadowsoft impermissibly use the information that it received? With each of these material factual questions still in dispute, a grant of qualified immunity to Defendants is inappropriate. *See Harrison v. Ash*, 539 F.3d 510, 517 (6th Cir. 2008) ("[T]o the extent that the denial of qualified immunity is based on a factual dispute, such a denial falls outside of the narrow jurisdiction of this Court.")

Secondly, the majority's reading of the DPPA not only contradicts the "straightforward and commonsense meaning[]" of the Act, *see Henry Ford Health Sys.*

---

[2] As this appeal arises from a motion for judgment on the pleadings, Defendants must concede all factual allegations to Plaintiffs. Therefore, if there were a dispute regarding whether Shadowsoft permissibly used the records it obtained from BMV Officials, Plaintiff's factual allegations must be conceded for the purposes of the qualified immunity inquiry. *See JPMorgan Chase Bank, N.A. v. Winget*, 510 F.3d 577, 581 (6th Cir. 2007) ("For purposes of a motion for judgment on the pleadings, all well-pleaded material allegations of the pleadings of the opposing party must be taken as true, and the motion may be granted only if the moving party is nevertheless clearly entitled to judgment.") (internal citations and quotation marks omitted).

v. Shalala, 233 F.3d 907, 910 (6th Cir. 2000), but if accepted also renders much of the language of the DPPA completely superfluous. *See Hibbs v. Winn*, 542 U.S. 88, 101 (2004) ("A statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant.") (citing 2A N. Singer, Statutes and Statutory Construction § 46.06, pp. 181-186 (rev. 6th ed. 2000)).

Under the majority's reading of the DPPA, the Act places no actual duty upon BMV Officials, other than the ministerial task of soliciting rote representations from prospective requesters. In the majority's view, as long as BMV Officials receive such rote representations, then they have complied with the DPPA.

It is difficult to reconcile this reading of the Act by the majority with the very next conclusion reached in its opinion. Because the majority continues by holding that even when a requestor does not provide a representation that it is acting in accordance with the DPPA—for instance, that the requester is a "legitimate business" under 18 U.S.C. § 2721(b)(3)—BMV Officials still do not violate the Act by knowingly disclosing information to that requestor.

The majority, in determining whether BMV Officials are liable to Plaintiffs because they disclosed information that was used for an impermissible purpose, holds that BMV Officials are immune because they disclosed the information in reliance on Shadowsoft's arguably false representations. But in determining whether BMV Officials are liable to Plaintiffs because they disclosed information to an arguably illegitimate business, the majority holds that BMV Officials are entitled to immunity, even though Shadowsoft made no actual representations that would invite the reliance of BMV Officials. Under this interpretation of 18 U.S.C. § 2721(b)(3), whether BMV Officials relied on false representations, *or none at all*, is of no actual consequence. The majority seemingly holds that the DPPA permits state officials such as those at the BMV to ask nothing and require no salient information, but to disclose everything.

Clearly, any interpretation of the DPPA that would require a requestor to make an affirmative statement of illegal intent or bad purpose in order for disclosure liability to attach to BMV Officials is inconsistent with both the language and the purpose of the

Act. While the DPPA may not mandate that BMV Officials conduct an actual investigation into an entity requesting drivers' information, or verify that entity's purpose, it clearly imposes some kind of duty upon the state and state officials. If it did not, then subjecting the state to a penalty for having a "policy or practice of substantial noncompliance" with the DPPA would be nonsensical, because as a practical matter a state (or its officials) could not fail to comply with an Act that imposes no actual duty upon it. *See* 18 U.S.C.A. § 2723(b).

Therefore, a proper reading of the DPPA compels the conclusion that the Act imposes upon the state (and its officials) a duty of reasonable inquiry. In this case, the permissible use that Defendants claim allows BMV Officials to knowingly disclose drivers' personal information to a certain type of requestor—"a legitimate business"—for certain purposes—"to verify the accuracy of personal information" and "to obtain . . . correct information" to prevent fraud or pursue other legal remedies. 18 U.S.C. § 2721(b)(3). Consequently, the Act sets forth a requirement that BMV Officials reasonably inquire into the dual questions of the identity of the requestor and the purpose for which information protected under the Act is being disclosed.

The content of the Record Request form ("Form 1173") created by BMV Officials to ensure compliance with the DPPA confirms that BMV Officials understood that the DPPA imposed this duty of reasonable inquiry. This understanding is apparent from the fact that Form 1173 requires that a requester submit both information about itself and information about the basis for the request. (*See* R. 13; Ex. A, B.)

On the two Form 1173s completed by Shadowsoft, the company provided none of the required information about itself, with the exception of an out-of-state mailing address. As the district court highlighted, "while [Form 1173] included places for Shadowsoft to provide its tax identification number, vendor number, professional license number, and license, Shadowsoft never completed this part of the form." (Dist. Ct. Op. at 21.) Nor did Shadowsoft provide any information regarding its status as a business in the contract that it subsequently entered into with BMV Officials, which did not request such information. (R. 13; Ex. A, B.)

Not inconsequently, it appears from the record that BMV Officials conducted this transaction with Shadowsoft via fax. So not only did BMV Officials not require Shadowsoft to represent that it was a licensed or incorporated business, it did not even require any actual contact with Shadowsoft. (*Id.*) There is no indication that BMV Officials even verified the identity of the individual requestor listed on the Form 1173s, Cara Hill, nor did she provide her personal driver license or social security number, as required by the forms. In practical terms, less verification was demanded of Shadowsoft, in order to receive the personal information of every driver in Ohio, than would be requested of any judge on this panel to write a personal check while shopping at any major retailer in this country.

The majority has strongly implied that Plaintiffs have somehow conceded that Shadowsoft operates as a "legitimate business," and that such a concession, if existent, should have some impact on this Court's legal analysis. (*See* Maj. Op. at p. 15.) On the contrary, Plaintiffs have alleged throughout the course of this litigation that BMV Officials had no basis for considering Shadowsoft a legitimate business at the time of the disclosure. (Pls.' Br. at 12-13, 22-23.) Defendants, in their answer to the complaint, denied any knowledge of Shadowsoft's corporate status based on their "want of information or knowledge sufficient to form a belief as to the truth of the matter." (R. 11: Answer at 3.) On reply before this Court, Defendants state that Shadowsoft is a legitimate business, but still offer no assertion or evidence that BMV Officials were aware of or inquired into this fact, even if accurate, at the time of the disclosure. (Defs.' Reply at 2-4.)

But whether Shadowsoft is a legitimate business is largely irrelevant.[3] What is relevant is that Defendants in this case do not plead that they knew or had any reason to believe that Shadowsoft was a legitimate business at the time that they made the

[3]Because the procedural posture of the case arises from a motion for judgment on the pleadings, no discovery was taken into the issue of Shadowsoft's claim that it was a "legitimate business" at the time that it made the record requests. Again, the majority's factual presumption that Shadowsoft was a "legitimate business," and that Defendants were in a position that would have allowed them to confirm as much, is misplaced. Because material disputes exist as to both of these questions, a grant of qualified immunity which relies upon accepting Defendants' representations on these matters is unjustified.

disclosure. At the time of the disclosure and alleged violation, Shadowsoft had neither represented itself to BMV Officials as a legitimate business, nor had BMV Officials inquired into or confirmed whether it was a legitimate business.

"The relevant, dispositive inquiry in determining whether a right is clearly established is whether it would be clear to a reasonable [official] that his conduct was unlawful in the situation he confronted." *Saucier v. Katz*, 533 U.S. 194, 202 (2001); *see also Cooper v. Parrish*, 203 F.3d 937, 951 (6th Cir. 2000). Even if it were true, as the majority contends, that BMV Officials' obligation of reasonable inquiry into a requester's permissible use begins and ends with a check in a box on a standardized form, it cannot be the case that a state official fulfills his legal obligations, under 18 U.S.C. § 2721(b)(3), when he releases drivers' personal information with absolutely nothing to indicate that he is releasing the information to a "legitimate business." Under the facts as pleaded in this case, any reasonable official would have been on notice that to disclose the information requested by Shadowsoft in response to Shadowsoft's facially deficient request would violate the DPPA.

Finally, it must be emphasized that the exceptions outlined in 18 U.S.C. §§ 2721(b)(1)-(14) are permissive, not mandatary. Holding that a state official must perform a reasonable minimal inquiry before releasing sensitive personal information to anyone with a fax machine, a pencil and two dollars does not impose an unreasonable burden. BMV Officials may decide that they do not want to face the threat of DPPA liability for disclosing drivers' information without first inquiring into whom and for what purpose they are being asked to disclose. The solution is simple: when in doubt as to whether the purpose of the request comports with the requirements of the Act, BMV Officials may choose not to release drivers' information for non-mandatory uses. After all, the purpose of the DPPA is to encourage state officials to do what they should strive to do anyway, which is to protect the personal information of state residents.

For these reasons, I would affirm the decision of the district court, and I therefore respectfully dissent from the opinion of the majority.