Cite as 2014 Ark. 139

SUPREME COURT OF ARKANSAS

No. CV-13-733

JON HOPKINS
APPELLANT

V.

THE CITY OF BRINKLEY, ARKANSAS; AND THE BRINKLEY WATER & SEWER DEPARTMENT
APPELLEES

Opinion Delivered April 3, 2014

APPEAL FROM THE MONROE COUNTY CIRCUIT COURT
[NO. CV-12-65]

HONORABLE L.T. SIMES II, JUDGE

REVERSED AND REMANDED.

JIM HANNAH, Chief Justice

Appellant, Jon Hopkins, appeals an order of the Monroe County Circuit Court finding that appellees City of Brinkley, Arkansas, and Brinkley Water & Sewer Department ("BW&S") were not required to disclose a municipal-utility ratepayer's home address under the Arkansas Freedom of Information Act (the "FOIA" or the "Act"), codified at Arkansas Code Annotated sections 25-19-101 to -110 (Repl. 2002 & Supp. 2011). We reverse and remand the circuit court's order.

A review of the record reveals that Hopkins submitted multiple requests to BW&S for the home address, phone number, and payment history of Kathryn Harris, a municipal-utility ratepayer and resident of Brinkley. BW&S responded by providing a redacted copy of her account history, which did not disclose her home address. In addition, BW&S stated that it "did not maintain the customer's telephone number." In denying the request for Harris's address, BW&S stated that it believed there was a "constitutional expectation of

private individuals not to have personal information disclosed publicly," that it considered a person's street address "to be something a person could expect to be a private matter not to be disclosed to third parties," and that "[r]ecent requirements of the adoption of identity theft protection measures by the Waterworks Department has further restricted the access of individuals to the information you request, even within the Waterworks Department." Hopkins appealed the denial of his request to the circuit court. After a hearing, the circuit court entered an order denying Hopkins's request, finding

> that [o]n October 27, 2008, the Brinkley Water and Sewer Commission adopted an Identify Theft Prevention Program, as required by 16 C.F.R. § 681.1(d)(1);
>
> that [Hopkins's] request for a customer's street address was denied by [BW&S] pursuant to the Brinkley Municipal Waterworks Identify Theft Prevention Program;
>
> that [BW&S has] provided [Hopkins] with account history information indicating the "requested individual" is a customer of the Waterworks Department and indicating the usage history of the customer, however, that personally identifiable information of the customer, including address, social security number, or other personal information has been redacted;
>
> that [BW&S's] providing of redacted information provides sufficient information to [Hopkins] to establish the conduct of a public function, as provided by the Freedom of Information Act of the State of Arkansas, while protecting the privacy of personal information as prescribed by the Identity Theft Prevention Program mandated by 16 C.F.R. § 681.1(d)(1); and
>
> [that BW&S is] not required to provide the street address or telephone number to [Hopkins] as requested.

Hopkins contends that the circuit court erred in finding that BW&S was not required to provide him with Harris's home address because a municipal-utility ratepayer's home address, a "public record" as defined by the FOIA, is not exempt from the Act's disclosure

and copying requirements. This court liberally interprets the FOIA to accomplish its laudable purpose that public business be performed in an open and public manner. *E.g.*, *Thomas v. Hall*, 2012 Ark. 66, at 4, 399 S.W.3d 387, 390. Furthermore, this court broadly construes the Act in favor of disclosure. *Id.*, 399 S.W.3d at 390. Arkansas Code Annotated § 25-19-105(a)(1)(A) (Supp. 2011) provides that "[e]xcept as otherwise specifically provided by this section or by laws specifically enacted to provide otherwise, all public records shall be open to inspection and copying by any citizen of the State of Arkansas during the regular business hours of the custodian of the records." Subsection (a)(2)(A) provides that "[a] citizen may make a request to the custodian to inspect, copy, or receive copies of public records." Ark. Code Ann. § 25-19-105(a)(2)(A) (Supp. 2011). Pursuant to subsection (d)(2)(A), "the custodian shall furnish copies of public records if the custodian has the necessary duplicating equipment," upon request and payment of a fee as provided in subsection (d)(3). Ark. Code Ann. § 25-19-105(d)(2)(A) (Supp. 2011).

We have held that for a record to be subject to the FOIA and available to the public, it must be (1) possessed by an entity covered by the Act, (2) fall within the Act's definition of a public record, and (3) not be exempted by the Act or other statutes. *E.g.*, *Nabholz Constr. Corp. v. Contractors for Pub. Protection Ass'n*, 371 Ark. 411, 416, 266 S.W.3d 689, 692 (2007). In this case, Hopkins and BW&S agree that BW&S is subject to the inspection and copying provisions of the FOIA and that the account history of a municipal ratepayer is a public record. BW&S and Hopkins part ways, however, on the issue of whether the ratepayer's home address is exempt from disclosure.

Hopkins contends that no exemption permits BW&S to withhold what is in the

public record. In support of his contention, Hopkins cites Arkansas Attorney General Opinion No. 2009-060, in which the Attorney General concluded that "[t]he individual payment records of customers of public utilities (such as water distributers under A.C.A. § 14-116-101 *et seq.*) are not eligible for any specific exemption under the FOA," Arkansas Attorney General Opinion No. 2000-129 (concluding that the FOIA "requires the disclosure of customer-specific payment-history records of a city-owned utility company"), and Arkansas Attorney General Opinion No. 97-244 (concluding that the FOIA requires disclosure of customer-specific payment-history records of a municipally owned water system). In addition, Hopkins points out that, in drafting the FOIA, the General Assembly exempted, for example, certain personnel records, *see* Ark. Code Ann. § 25-19-105(b)(12) (Supp. 2011) (stating that personnel records are not open to the extent that disclosure would constitute a clearly unwarranted invasion of personal privacy),[1] the personal contact information of certain government employees, *see* Ark. Code Ann. § 25-19-105(b)(13) (Supp. 2011) (stating that personal contact information, including home addresses of certain government employees contained in employee records, is not open, except that the custodian of the records shall verify an employee's city or county of residence or address on record

[1]At one time, the clearly-unwarranted-invasion-of-privacy exemption was not limited to personnel records. Rather, *any* information that, if disclosed, would constitute a clearly unwarranted invasion of privacy was not considered to be a part of the public record. In 1981, the General Assembly amended the definition of "public records," to include the following language: "Provided, that compilations, lists, or other aggregations of information of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy, are hereby determined to be confidential and shall not be considered to be 'public records' within the terms of this Act, and shall not be supplied to private individuals or organizations." *See* Act of Mar. 23, 1981, No. 608, § 3, 1981 Ark. Acts 1345, 1346 (1981). But that language was deleted in 1985. *See* Act of Mar. 21, 1985, No. 468, § 3, 1985 Ark. Acts 917, 918 (1985).

upon request), and certain concealed handgun records, *see* Ark. Code Ann. § 25-19-105(b)(19), as amended by Act 145 of 2013 (deleting (b)(19)(C), which stated that "[t]he name and the corresponding zip code of an applicant, licensee, or past licensee may be released upon request by a citizen of Arkansas"). Hopkins contends that because the ratepayer's home address is not exempt from disclosure by the Act, BW&S must disclose the information upon request.

BW&S agrees that there is no specific statutory exemption for a ratepayer's home address, but it contends that the Federal Trade Commission's Red Flags Rule preempts the FOIA's disclosure requirements. The Red Flags Rule requires certain companies to "develop and implement a written Identify Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account." 16 C.F.R. § 681.1(d)(1).

As required by federal regulations, BW&S developed an "Identity Theft Prevention Program," which BW&S says was "intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events." As part of the Program, BW&S implemented "Personal Information Security Procedures" with the aim of better protecting personal customer information. Procedures included storing files with "secure information" in locked file cabinets and limiting access to a customer's "personal identify [sic] information" to employees with a "need to know."

The Supremacy Clause of the United States Constitution provides that state laws that

"interfere with, or are contrary to the laws of Congress, made in pursuance of the constitution" are invalid. *Gibbons v. Ogden*, 22 U.S. 1, 210–11 (1824); U.S. Const. art. VI, cl. 2. State law is preempted under the Supremacy Clause in three circumstances: (1) when Congress makes its intent to preempt state law explicit in statutory language; (2) when state law regulates conduct in a field that Congress intends for the federal government to occupy exclusively; or (3) when there is an actual conflict between state and federal law. *English v. Gen. Elec. Co.*, 496 U.S. 72, 78–79 (1990).

BW&S contends that the third circumstance, an actual conflict, is present in the instant case because the FOIA, on its face, mandates disclosure of the same personal information that the Red Flags Rule and the Identity Theft Prevention Program seek to protect. BW&S contends that the federal law, which aims to protect a customer's personal information as a guard against identity theft, is incompatible with the FOIA, which would otherwise require the public disclosure of a customer's personal information.

The Supreme Court of the United States has explained that

> state law is pre-empted to the extent that it actually conflicts with federal law. Thus, the Court has found pre-emption where it is impossible for a private party to comply with both state and federal requirements or where state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.

English, 496 U.S. at 79 (internal quotations and citations omitted).

We are not persuaded by BW&S's contention that the FOIA is "incompatible" with the federal regulations that require BW&S to implement policies to detect, prevent, and mitigate identity theft. Pursuant to the federal regulations, "[i]dentity theft means a fraud committed or attempted using the identifying information of another person without

authority." 12 C.F.R. § 1022.3(h). "Identifying information" is defined as any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

> (1) Name, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
>
> (2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
>
> (3) Unique electronic identification number, address, or routing code; or
>
> (4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

12 C.F.R. § 1022.3(g).

Absent from the definition of "identifying information" is a person's home address. We recognize that 12 C.F.R. § 1022.3(g) does not contain an exhaustive list of names and numbers that qualify as "identifying information," but we do not agree with BW&S's contention that, to prevent and mitigate identity theft, a person's home address is considered to be "within the same family" of the other items listed in the definition or that a person's home address is akin to a person's Social Security number or date of birth.[2] We conclude that

---

[2] *See, e.g.*, *Office of Lieutenant Governor v. Mohn*, 67 A.3d 123, 132 (Pa. Commw. Ct. 2013) (recognizing the "'Holy Trinity' of personal information, i.e., person's name, social security number and date of birth, that are reasonably likely to result in identity theft and fraud," and concluding that sufficient proof had not been presented to add "home address" to the "Holy Trinity"); *Governor's Office of Admin. v. Purcell*, 35 A.3d 811, 813 (Pa. Commw. Ct. 2011) (crediting an identity theft, privacy, and security expert's affidavit testimony that the "Holy Trinity . . . can be used by identity thieves to establish new financial accounts in the name of the identity theft victim and to commit a variety of other types of identity fraud. While one cannot hold one's name secret, one can often protect their Social Security number and date of birth. . . . Organizations that maintain records that contain consumer date of births must protect that personal identifier and other personally identifiable

the FOIA is not preempted by the Red Flags Rule because the laws do not conflict.

BW&S next contends that the Arkansas Constitution protects a municipal-utility customer's individual privacy rights, including the secrecy of his or her personal information. In support of this argument, BW&S cites *McCambridge v. City of Little Rock*, 298 Ark. 219, 766 S.W.2d 909 (1989), in which this court recognized "a constitutional right to nondisclosure of personal matters." *Id.* at 229, 766 S.W.2d at 914 (citing *Whalen v. Roe*, 429 U.S. 589 (1977)). In that case, McCambridge's son, John Markle, committed suicide after having murdered his wife and child, and the Little Rock Police Department recovered several items from the crime scene, including two handwritten letters from Markle to his attorney, a diary containing Markle's notes, a handwritten letter from Markle to McCambridge, and miscellaneous notes. McCambridge filed suit against the City of Little Rock and its police department, seeking to restrain the department from releasing to the media the items listed above and the crime-scene photographs.

The court noted that McCambridge had a right "to avoid disclosure by the government of some personal matters," *id.* at 230, 766 S.W.2d at 914, and concluded that a constitutional privacy interest applies to matters "(1) that the individual wants to [keep] and has kept private or confidential, (2) that, except for the challenged government action, can be kept private or confidential, and (3) that to a reasonable person would be harmful or

---

information that the consumer entrusted with the organization.").

BW&S's Identity Theft Prevention Program contains "Personal Information Security Procedures" that refer to "secure information," "personally identifiable information," "sensitive information," "sensitive consumer data," "sensitive data," and "personally identify [sic] information." None of those terms are defined.

embarrassing if disclosed." *Id*. at 230, 766 S.W.2d at 914 (citing Bruce E. Falby, Comment, *A Constitutional Right to Avoid Disclosure of Personal Matter: Perfecting Privacy Analysis in* J.P. v. DeSanti, 653 F.2d 1080 (6th Cir. 1981), 71 Geo. L.J. 219, 240 (1981)). Having determined which items involved "personal matters," pursuant to the three-part test, the court then considered "whether the governmental interest in disclosure under the Freedom of Information Act outweighs the appellant's privacy interest in the nondisclosure of the personal matters." *Id*. at 231, 766 S.W.2d at 915 (citing *Nixon v. Admin. of Gen. Servs.*, 433 U.S. 425, 458 (1977)). Ultimately, the court concluded that the governmental interest in disclosure under the FOIA outweighed McCambridge's privacy interest in nondisclosure. *Id*. at 231–32, 766 S.W.2d at 915.

BW&S contends that a home address qualifies as a "personal matter" under *McCambridge* and is thus "constitutionally protectable" because it is the type of information that an individual wants to keep and has kept private or confidential, except for its potentially being released pursuant to a FOIA request; it is a class of information that an individual can keep private and confidential; and a reasonable person would find the disclosure of such information harmful. BW&S further contends that, because an individual's interest in protecting his or her personal information is substantial and because there is "little to no relevant" public interest in a municipal-utility customer's personal information, the personal information should not be disclosed.

The Tennessee Court of Appeals recently addressed a similar argument. In *Patterson v. Convention Center Authority of Metro Government of Nashville*, No. M2012-00341-COA-R3-CV, 2013 WL 209051 (Tenn. Ct. App. Jan. 17, 2013), the Convention Center Authority

("CCA") appealed the trial court's determination that the residential addresses of employees of third-party contractors contained in payroll records submitted by the contractors to the Convention Center Authority were not exempt from disclosure under the Tennessee Public Records Act ("TPRA"). After concluding that the TPRA did not prohibit disclosure of the addresses, the Tennessee Court of Appeals addressed the CCA's contention that workers had constitutional privacy rights to prevent disclosure to their home addresses:

> The CCA additionally asserts that workers have constitutional privacy rights to nondisclosure of their home addresses, and that disclosure of residential addresses under the TPRA would violate this right. Petitioners assert that the CCA lacks standing to assert this issue. In *Schneider v. City of Jackson*, the supreme court stated that the City of Jackson had failed to demonstrate that it had standing to assert the privacy rights of individuals where the cases upon which it relied were filed by the individuals alleging constitutional violations. *Schneider v. City of Jackson*, 226 S.W.3d 332, 344 n. 16 (Tenn. 2007). The *Schneider* court additionally stated:
>
> were we to assume that the City has standing to assert the constitutional claim, the City has failed to offer specific proof that disclosing the field interview cards would threaten the personal security and bodily integrity of certain interviewees, proof that is necessary to establish such a claim.
>
> *Id*.
>
> . . . .
>
> As in *Schneider*, Petitioners here have failed to demonstrate that they have standing to assert the individual workers' constitutional privacy rights. Additionally, as in *Schneider*, Petitioners here have offered no proof that disclosing the workers' addresses would threaten the personal security or bodily integrity of any worker. We accordingly decline to address this issue.

Patterson, 2013 WL 209051, at *14.

In the instant case, BW&S relies on *McCambridge*, a case in which an individual alleged constitutional violations of privacy, to assert the privacy rights of all its customers. Even if we

were to assume that BW&S has standing to assert the constitutional claim, it has failed to offer specific proof that any customer's home address qualifies as a "personal matter" under the standards set forth in *McCambridge*. Therefore, we decline to address BW&S's privacy argument. *See Patterson*, *supra*; *see also* Op. Ark. Att'y Gen. No. 285 (2002) (stating that any records maintained by a water district reflecting the names, addresses, and telephone numbers of its paying customers constitute "public records" that are not exempt from disclosure, but recognizing that, in some cases, unlisted telephone numbers and unlisted addresses may meet the *McCambridge* standards).

BW&S also contends that Hopkins's request for a municipal ratepayer's home address falls outside of the FOIA's stated purpose and, therefore, the address should not be disclosed. The legislative intent of the FOIA is stated in Arkansas Code Annotated section 25-19-102 (Repl. 2002):

> It is vital in a democratic society that public business be performed in an open and public manner so that the electors shall be advised of the performance of public officials and of the decisions that are reached in public activity and in making public policy. Toward this end, this chapter is adopted, making it possible for them, or their representatives to learn and to report fully the activities of their public officials.

BW&S asserts that the home address of a public-utility customer should not be disclosed because the disclosure will not aid anyone in evaluating the operation and performance of the public utility and the job performance of the public officials responsible for running the public utility. But BW&S points to no law that requires a citizen to give a reason for his or her request to inspect public records. The FOIA does not direct itself to the motivation of the person who seeks public records. *See* John J. Watkins & Richard J. Peltz,

The Arkansas Freedom of Information Act 410 (Ark. Law Press, 5th ed. 2009) (noting that under the Act, "any public record that is not specifically exempt from disclosure is available for inspection and copying by any citizen of the State of Arkansas, irrespective of his purpose or motive in seeking access") (internal quotations and footnote omitted).

Finally, BW&S makes a policy argument, stating that

> the personal contact information, including home address and personal email address, of a public employee is specifically exempted from disclosure under FOIA. Ark. Code Ann. § 25-19-105(b)(13). In other words, a BW&S employee's home address would be exempt from disclosure pursuant to a FOIA request. It defies logic that a private customer of a public utility, who has no connection to the operation of the public utility, should receive less protection than an employee of a public utility, who is supported by the taxpayers, when it comes to the protection of his or her personal information.

Whether certain records should be exempt from the FOIA is a public-policy decision that must be made by the General Assembly and not the courts. *E.g.*, *Harris v. City of Fort Smith*, 359 Ark. 355, 365, 197 S.W.3d 461, 467 (2004). As we noted in *City of Fayetteville v. Edmark*, 304 Ark. 179, 194–95, 801 S.W.2d 275, 283 (1990), it is the job of the General Assembly to establish exemptions under the FOIA, and arguments for additional exemptions must be addressed to the General Assembly because this court "can only interpret the exemption as it is written." *Id.* (citing *McCambridge*, 298 Ark. at 233, 766 S.W.2d at 916).

Reversed and remanded.

HOOFMAN, J., dissents.

CLIFF HOOFMAN, Justice, dissenting. I must respectfully dissent. The majority's decision has the effect of requiring the disclosure of the home address of every resident of every community of this state who subscribes to the services of any public utility (water,

sewer, cable television, electricity, solid waste, and recycling services, etc.). I do not believe that the legislature intended such a result. Personal information such as a ratepayer's home address or phone number has no relation to the stated purpose of the Freedom of Information Act (FOIA), which is to make it possible for electors "to learn and to report fully the activities of their public officials." Ark. Code Ann. § 25-19-102 (Repl. 2002). While I recognize that the FOIA is broadly construed in favor of disclosure and that exceptions to the Act are narrowly construed, we have also stated that "we will balance the laudable interest in favor of disclosure with the intent of the General Assembly and do so with a common sense approach." *Byrne v. Eagle*, 319 Ark. 587, 590, 892 S.W.2d 487, 488 (1995); *see also Sebastian Cnty. Chapter of the Am. Red Cross v. Weatherford*, 311 Ark. 656, 846 S.W.2d 641 (1993); *Bryant v. Mars*, 309 Ark. 480, 830 S.W.2d 869 (1992). Given that the General Assembly exempted from disclosure the personal contact information of employees of these public utilities, pursuant to Ark. Code Ann. § 25-19-105(b)(13) (Supp. 2013), it defies logic and common sense to conclude that this same information concerning a public utility's private customers was intended to be disclosed under the Act. These customers often are required to subscribe to the services of such utilities in order to be a resident of that community and thus would have no choice but to have their private contact information disclosed. The legislature surely did not foresee such an absurd result and therefore saw no need to enact a specific exception for the utilities' customers, as it did for the utilities' employees. Thus, I would affirm the circuit court's order.

Joseph Hamilton Kemp, PLLC, by: *Joseph Hamilton Kemp*, for appellant.

Raymond R. Abramson and *John W. Martin*, for appellees.