

[J-173-2002]
IN THE SUPREME COURT OF PENNSYLVANIA
EASTERN DISTRICT

COMMONWEALTH OF PENNSYLVANIA,	:	No. 50 E.D. Appeal Docket 2000
	:	
Appellee,	:	Appeal from the Order of the Superior
	:	Court dated April 4, 2000, reversing the
v.	:	January 5, 1998 Order of the Court of
	:	Common Pleas of Philadelphia County
	:	
	:	752 A.2d 404 (Pa. Super. 2000)
DAVID DUNCAN,	:	
	:	
Appellant.	:	RESUBMITTED: August 22, 2002
	:	
	:	
	:	
	:	

OPINION

MR. JUSTICE CASTILLE

DECIDED: March 4, 2003

This Court granted limited discretionary review of a pretrial suppression ruling to consider whether a warrantless telephone call police made to appellant's bank, seeking the name and address information associated with an Automatic Teller Machine card ("ATM card") used by a person suspected of rape, violated appellant's rights under Article 1, Section 8 of the Pennsylvania Constitution. Because we hold that the telephone call did not violate appellant's rights, we affirm the Superior Court.

The facts demonstrated that at approximately 6:00 p.m. on November 10, 1996, a male unknown to the victim approached her as she was walking near the street lit intersection of 20th Street and John F. Kennedy Boulevard in Philadelphia. The male asked

the victim if she was "working." The victim answered "no" and continued walking. A short time later, the same male confronted the victim a second time, this time claiming to have a gun in his coat pocket and threatening to kill her if she did not do as she was told. He then grasped the victim by the arm and forced her to an enclosed space beneath nearby train tracks where he raped her and stole her money.

The victim immediately reported the assault to the police and described her assailant as a white male, 27 to 28 years old, approximately six feet tall, weighing 210 to 220 pounds, of medium build, with light brown hair, and wearing a puffy, dark green Philadelphia Eagles jacket and blue jeans. Later that night, the police canvassed stores near the crime scene. The cashier at a pornography store, Elgee's Novelty Shop, told the police that a man matching the victim's description of the assailant had been in the store around the time of the rape and that this man had attempted to make a purchase using an ATM card, but the card was rejected. The cashier provided the police with a list maintained by the shop of all ATM card transactions attempted and completed that day. The list showed the number of each card used and identified the bank that issued the card. The list indicated that two different ATM cards -- one issued by Mellon Bank and one issued by Drovers and Mechanics Bank ("Drovers Bank") -- had been rejected. The police also viewed the store's surveillance videotape, which showed a man matching the victim's description of her assailant attempting to make a purchase with an ATM card.

Thereafter, the police served a search warrant on Mellon Bank to obtain, *inter alia*, the name, address, and telephone information corresponding to the declined Mellon Bank ATM card. Mellon Bank provided this information, and the user of the card was ultimately eliminated as a suspect. The police then telephoned Robert Garrison, the manager of Drovers Bank, and requested the name and address corresponding to the declined Drovers Bank ATM card. The police inexplicably did not obtain a warrant before making this telephone request. Mr. Garrison consulted a list, kept within the bank, of all individuals to

whom the bank had issued ATM cards. Mr. Garrison then relayed to police appellant's name and address in York County, Pennsylvania. Mr. Garrison did not ask the police if they had a warrant because the information requested by the police "was not financial." N.T. 9/29/1997 at 15.

On March 1, 1997, the police executed a search warrant for samples of appellant's blood, bodily fluid, and hair. On March 14, 1997, police arrested appellant pursuant to a warrant and charged him with rape and related offenses. According to the arrest warrant, DNA testing of the samples taken pursuant to the search warrant linked appellant to the alleged rape to a probability of over 99.99%. The victim later failed to identify appellant from a photographic array. At a subsequent in-person line-up, however, the victim identified appellant as the person who had attacked her.

Appellant filed a motion to suppress, in relevant part, the blood, bodily fluid, and hair samples, as well as the victim's line-up identification. Appellant contended, *inter alia*, that he had a state constitutional right of privacy in the name and address information disclosed by his bank to the police under this Court's decision in Commonwealth v. DeJohn, 403 A.2d 1283 (Pa. 1979), cert. denied, 444 U.S. 1032 (1980). Appellant asserted that the police violated this privacy right by telephoning his bank and requesting this information without first obtaining a warrant, and that the biological samples, DNA results, and identification evidence should be suppressed as the constitutionally-tainted fruit of the illegal telephone call.

A hearing was held on this motion on September 29, 1997. In addition to the Commonwealth's evidence, appellant himself briefly testified and admitted that he came to Philadelphia on the date of the crime in question to purchase an Eagles jacket, and that after purchasing the jacket he wore it for "the entire day and the entire night." N.T. 9/29/1997 at 89. Appellant never testified whether he believed that his bank would keep

his name and address private, nor did he present any evidence from his bank suggesting what level of privacy, if any, it promised its customers.

The Honorable Gregory E. Smith, of the Court of Common Pleas of Philadelphia County, granted the motion to suppress. The court held that the name and address information requested by the police and disclosed by appellant's bank were constitutionally-protected "bank records" within the purview of DeJohn. Since the suppression court read DeJohn as authorizing the "acquisition" of bank records only pursuant to a valid warrant, and since the police here did not obtain a search warrant before requesting the name and address corresponding to the ATM card number from Drovers Bank, the suppression court concluded that the police illegally seized the information by asking for it telephonically. Appellant's blood, bodily fluid, and hair samples, as well as the DNA test results and the victim's positive line-up identification, were suppressed as the tainted fruits of this unconstitutional telephone call.¹

Upon the Commonwealth's certified appeal,² a unanimous panel of the Superior Court reversed in a published opinion authored by the Honorable Kate Ford Elliott. Commonwealth v. Duncan, 752 A.2d 404 (Pa. Super. 2000). The Superior Court focused on whether appellant had an expectation of privacy in his bank's knowledge of his name

¹ The suppression court also held that the prosecution's failure to inform appellant prior to the line-up that the victim had previously failed to identify his picture from a photographic array was prosecutorial misconduct which denied the defense a fair opportunity to avoid a suggestive line-up identification. The court suggested that the line-up identification could have been suppressed on this basis, but determined that it "need not reach this issue because the line-up identification was a fruit of the initial invasion of private bank records." Slip op. at 6. On appeal, the Superior Court reversed the suppression court's finding of prosecutorial misconduct. This Court declined discretionary review of this issue.

² The Commonwealth certified that the suppression court's order would effectively terminate or substantially handicap the prosecution, thus perfecting its right to appeal the pretrial order. PA.R.A.P. 311(d); Commonwealth v. Templin, 795 A.2d 959, 961 n.3 (Pa. 2002); Commonwealth v. Dugger, 486 A.2d 382, 386 (Pa. 1985).

and address. Following a thorough discussion of DeJohn and other precedents from this Commonwealth, as well as a number of decisions from other jurisdictions, the Superior Court observed that "there is a fundamental difference between the type of information that is subject to a constitutionally protected right to privacy and a person's identification information, *i.e.*, one's name and address." 752 A.2d at 412. The type of information that "is deserving of constitutional protection," the court continued, consists "of the unique, perhaps controversial or unpopular, essence of one's personality rather than merely identifying individuals, where they live, and their telephone number." Id. Thus, the Superior Court concluded that "a person's name and address, by themselves, do not constitute information about which a person can have a reasonable expectation of privacy that society is willing to recognize." Id., quoting State v. Chryst, 793 P.2d 538, 542 (Alaska Ct. App. 1990). Because the name and address information disclosed to the police by the bank did not fall within the scope of information protected by Article I, Section 8, the Superior Court held that the police did not violate the Pennsylvania Constitution in requesting this information without first obtaining a warrant.

This Court granted limited review to consider whether appellant had a reasonable expectation of privacy in the name and address information provided by his bank to the police under Article I, Section 8 of the Pennsylvania Constitution and our decision in DeJohn. Article I, Section 8 provides:

The people shall be secure in their persons, houses, papers and possessions from unreasonable searches and seizures, and no warrant to search any place or to seize any person or things shall issue without describing them as nearly as may be, nor without probable cause, supported by oath or affirmation subscribed to by the affiant.

Pa. Const. Art I, § 8. This Court has "accorded greater protections to the citizens of this state under Article I, Section 8 of our constitution under certain circumstances," but we have also recognized that that fact "does not command a reflexive finding in favor of any

new right or interpretation asserted." Commonwealth v. Glass, 754 A.2d 655, 660 (Pa. 2000), quoting Commonwealth v. Cleckley, 738 A.2d 427, 431 (Pa. 1999). See also In re D.M., 781 A.2d 1161, 1163 (Pa. 2001) (declining to depart from Terry v. Ohio, 392 U.S. 1 (1968) and progeny). Because we find that this Court's decision in DeJohn does not support the suppression court's legal conclusion that appellant had a right of privacy in the mere name and address information disclosed by his bank, and because we find that this Court's Article I, Section 8 jurisprudence should not be expanded to encompass such a circumstance, we affirm the Superior Court.

In reviewing a suppression ruling, this Court is bound by the suppression court's factual findings which find support in the record, but we are not bound by the court's conclusions of law. Commonwealth v. Templin, 795 A.2d 959, 961 (Pa. 2002) (citations omitted). The question before us involves undisputed facts. The legal issue is whether appellant had a reasonable expectation of privacy under the Pennsylvania Constitution in the name and address information disclosed by his bank. This is a conclusion of law and, as such, is subject to plenary review. See Commonwealth v. Glass, 754 A.2d 655, 658 (Pa. 2000).³

³ Preliminarily, we note that appellant has not briefed and analyzed his state constitutional claim pursuant to the standards set forth in Commonwealth v. Edmunds, 586 A.2d 887, 895 (Pa. 1991) ("[A]s a general rule it is important that litigants brief and analyze at least the following four factors: 1) text of the Pennsylvania constitutional provision; 2) history of the provision, including Pennsylvania case-law; 3) related case-law from other states; 4) policy considerations, including unique issues of state and local concern, and applicability within modern Pennsylvania jurisprudence."). Although the failure to engage in an Edmunds analysis is not fatal to a claim under the Pennsylvania Constitution, we strongly encourage the use of that framework. See Commonwealth v. Swinehart, 664 A.2d 957, 961 n.6 (Pa. 1995); see also Commonwealth v. Arroyo, 723 A.2d 162, 166 n.6 (Pa. 1999). For our purposes, since DeJohn (which preceded Edmunds) is the leading case and was decided under Article I, Section 8, there is no need to further discuss the first two Edmunds factors. To the extent the other factors are relevant, they are discussed *infra*.

Since the proper interpretation of DeJohn is our primary task, we begin with a discussion of that case. In DeJohn, the appellant was suspected of murdering her husband in order to collect the proceeds of his life insurance policy, of which she was the primary beneficiary. In an effort to obtain evidence of a financial motive for the crime, the local District Attorney's Office served two "court subpoenas" on officials of the bank where appellant and/or her husband were believed to maintain one or more accounts. The "subpoenas" were obtained without any court process. Indeed, the DeJohn Court noted that at the time both "subpoenas" were issued there was no ongoing legal proceeding of any nature. Thus, no Common Pleas Court Judge or District Justice had issued or authorized the "subpoenas." Instead, they bore the signature of the local Clerk of Courts.

The first "subpoena" demanded "copies of all information pertaining to accounts, or application for account, made by Jill and/or Michael DeJohn." The second "subpoena" demanded "all original records pertaining to personal cash reserve account application, and original new account card for Michael and Jill DeJohn." Pursuant to these "subpoenas," the police obtained the actual cancelled check used to purchase the typewriter that Jill DeJohn had used to type an extortion note to a neighbor. In addition, the police obtained evidence that DeJohn had signed her husband's signature on a loan application to obtain money to pay back \$3,000 owed to an employee of their home builder. This evidence of DeJohn's financial dealings, secured by police employing non-legal subpoenas, was introduced at her murder trial to show motive and she was ultimately convicted of third-degree murder. In a subsequent trial, DeJohn was also convicted of attempted theft by extortion concerning her neighbor.

On appeal, DeJohn argued that the subpoenas were unlawful and were used to procure evidence and that the evidence seized should be suppressed. The Commonwealth did not dispute that the subpoenas were illegal; and this Court noted that, under our precedent, the Commonwealth could not claim that the subpoenas were lawful.

403 A.2d at 1287 n.5. Instead, the Commonwealth argued that DeJohn lacked standing to challenge the concededly illegal seizure of the bank records. This Court noted that the question of whether a depositor has standing to challenge the seizure of bank records was one of "first impression in this court." 403 A.2d at 1287. On the standing question, the Commonwealth relied on the United States Supreme Court's then-recent decision in United States v. Miller, 425 U.S. 435 (1976), which held that bank depositors do not have a reasonable expectation of privacy in their bank records.

This Court reversed DeJohn's murder conviction and granted a new trial, finding that the trial court erred in admitting the bank records seized pursuant to the invalid subpoenas.⁴ On the standing question, the Court acknowledged the reasoning in Miller that a bank customer does not have a Fourth Amendment interest in his bank records because the bank customer assumes the risk that in revealing his financial affairs to the bank and its employees that this information may then be conveyed to the Government.

⁴ The Commonwealth is technically correct in referring to DeJohn as a plurality opinion. Justice O'Brien's lead opinion in DeJohn was joined outright by only two of the five other participating Justices: Chief Justice Eagen and Justice Nix. Justice Pomeroy did not participate. Justice Roberts filed a concurring opinion in which, among other things, he expressed disagreement with the lead opinion's Article I, Section 8 analysis since, in his view, a bank customer's interest in his account is "something less than a constitutional right of privacy." 403 A.2d at 1293 (Roberts, J., concurring). Justice Larsen filed a concurring and dissenting opinion, expressing his view that a depositor has no reasonable expectation of privacy in bank records. 403 A.2d at 1293-94 (Larsen, J., concurring and dissenting). The fourth vote for the Article I, Section 8 holding was provided by the dissent of Justice Manderino. The dissent would have discharged DeJohn on the murder charge on sufficiency grounds. On the Article I, Section 8 question, Justice Manderino did not join the lead opinion, but stated that, "[t]he bank records, must be excluded for the reasons stated by the majority with which I agree." 403 A.2d at 1307 (Manderino, J., dissenting). In light of the specific comments of Justice Manderino, it is clear that four Justices were in agreement that, under Article I, Section 8 of the Pennsylvania Constitution, DeJohn had a legitimate expectation of privacy in the records that were seized via the bogus subpoenas. There is, then, a clear mandate regarding the expectation of privacy in those sorts of records. For this reason, and for ease of exposition, we will refer to Justice O'Brien's opinion as the opinion of the Court.

The DeJohn Court noted, however, that "the state has the power to impose standards on searches and seizures higher than those required by the Federal Constitution." DeJohn, 403 A.2d at 1288, quoting Commonwealth v. Harris, 239 A.2d 290, 292 n.2 (Pa. 1968). The Court found that "Miller establishes a dangerous precedent, with great potential for abuse, [and] decline[d] to follow the case when construing the state constitutional protection against unreasonable searches and seizures." Id.

The Court did not cite anything unique to Pennsylvania constitutional doctrine in justification of its departure from Miller on the question of privacy expectations in bank records. Instead, the Court primarily found guidance on the substantive question in the decision of the California Supreme Court in Burrows v. Superior Court, 529 P.2d 590 (Cal. 1974). Burrows considered this same issue under the California Constitution. The Court quoted extensively from Burrows, including the California Supreme Court's observations that:

For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography. While we are concerned in the present case only with bank statements, the logical extension of the contention that the bank's ownership of records permits free access to them by any police officer extends far beyond such statements to checks, savings, bonds, loan applications, loan guarantees, and all papers which the customer has supplied to the bank to facilitate the conduct of his financial affairs upon the reasonable assumption that the information would remain confidential. To permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power.

Cases are legion that condemn violent searches and invasions of an individual's right to the privacy of his dwelling. The imposition upon privacy, although perhaps not so dramatic, may be equally devastating when other methods are employed. Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new devices.

DeJohn, 403 A.2d at 1289-90, quoting Burrows, 529 P.2d at 596.

Finding the analysis of the California Supreme Court "in recognizing modern electronic realities" to be "more persuasive than the simplistic proprietary analysis . . . used by the Court in Miller," the DeJohn Court "adopt[ed]" its reasoning. Id. at 1290-91. Accordingly, the Court ruled that "under Article I, Section 8 of the Pennsylvania Constitution bank customers have a legitimate expectation of privacy in records pertaining to their affairs kept at the bank." Id. at 1291. The Court then held that, "[s]ince the records seized in the instant case were taken pursuant to an invalid subpoena, and appellant had a legitimate expectation of privacy in those records, appellant has standing to challenge their admissibility." Id.⁵

Echoing the view of the suppression court, appellant contends that the police request here implicated his "bank records" in which he had a reasonable expectation of privacy under DeJohn. The dissent likewise asserts that this case "involves account

⁵ It should be noted that DeJohn was decided before this Court held, in Commonwealth v Sell, 470 A.2d 457 (Pa. 1983), that a defendant charged with a possessory offense has automatic standing under Article I, Section 8 to challenge the lawfulness of the seizure of evidence relating to the possessory charge. Sell's automatic standing rule would have no effect in a case, such as DeJohn or the case *sub judice*, where the defendant is not charged with a possessory offense. The inquiry whether a defendant has a reasonable expectation of privacy for standing purposes, in a non-possessory offense case, is no different from the inquiry when analyzing whether police conduct involves a recognized zone of privacy.

information that was provided to police along with a name and address." Dissenting slip op. at 6. In actuality, however, as the Commonwealth notes, the police did not request, nor did the bank reveal, anything of the kind. The police asked the bank only for the name and address that corresponded to the suspected rapist's ATM card number -- which the police had already obtained from a third party -- and the bank gave them **only** that information. The police here did not gain "unbridled" access to all of appellant's bank records "without any judicial control as to relevancy or other traditional requirements of legal process." DeJohn, 403 A.2d at 1290, quoting Burrows, 529 P.2d at 593, 596. The police did not request, nor did they review, **any** of appellant's "bank statements," "checks," "savings," "bonds," "loan applications," "loan guarantees," or any of the other "papers which [a] customer . . . supplie[s] to the bank to facilitate the conduct of his financial affairs." Id. Indeed, it appears the police received no documents at all, but instead were simply provided appellant's name and address in a telephone conversation with the bank manager. Police did not seek evidence of a crime reposing hidden within the bank's financial documents. Rather, they were looking for the mere **identity** of the person they had strong reason to believe had forcibly raped a woman, and who had attempted to use a precisely identified ATM card. To that end, they telephoned appellant's bank, and were told his name and address. Appellant's protestations notwithstanding, it is simply inaccurate for him to assert that his bank records were requested or disclosed in this case.

The disclosure of a mere name and address corresponding to a particular ATM card number is obviously different in kind from the disclosure of substantive bank records that was the subject of the standing decision in DeJohn. A person's name and address do not, by themselves, reveal anything concerning his "personal affairs, opinions, habits or associations." Such innocuous information does not provide or complete a "virtual current biography." A noted criminal procedure expert -- who happens to agree with this Court's conclusion in DeJohn that the result reached by the United States Supreme Court in Miller

was "dead wrong" in its determination of privacy expectations in bank records -- has observed:

Admittedly, it cannot be said that all information about a person is private in the Fourth Amendment sense. . . . [W]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection, and certainly some of the information which institutions collect in the course of business transactions fit that description. For example, if law enforcement agents were allowed to consult business records which merely revealed a person's name or address or telephone number, this does not offend any interests protected by the Fourth Amendment. . . . But bank records are another matter, for unquestionably they can reveal much about a person's activities, associations, and beliefs.

Wayne R. LaFave, Search and Seizure (3d ed. 1996), § 2.7(c), at 633 (footnotes, citations, and internal quotation marks omitted). That appellant's mere name and address happened to have been obtained from a bank, as opposed to some other source, does not somehow transform this identifying information into the kind of revealing financial data "which a person [would] normally choose[] to exclude from prying eyes and inquisitive minds" that led this Court to diverge from Fourth Amendment precedent in DeJohn.

DeJohn, in short, does not support the conclusion that appellant had a right of privacy as a matter of law in the name and address information verbally disclosed by his bank to the police. Moreover, appellant has failed to persuade us that this Court's Article I, Section 8 jurisprudence should be expanded to encompass this new circumstance. In determining the scope of protection afforded under Article I, Section 8, this Court employs the same two-part test employed by the United States Supreme Court to determine the sweep of the Fourth Amendment of the U.S. Constitution -- a test first articulated by Justice Harlan in his concurring opinion in Katz v. United States, 389 U.S. 347 (1967). See, e.g., Commonwealth v. Rekasie, 778 A.2d 624, 629 (Pa. 2001). "That test requires a person to

(1) have established a subjective expectation of privacy and (2) have demonstrated that the expectation is one that society is prepared to recognize as reasonable and legitimate." Commonwealth v. Gordon, 683 A.2d 253, 256 (Pa. 1996).

Appellant contends that in our "increasingly complex, technological society" it is "eminently reasonable" for an individual to expect that "his right to privacy in his bank records extends to his name and address." Brief for Appellant at 16. He argues that the increased use of computers and other sophisticated technology to store personal information has greatly magnified the potential risks to individual privacy. See id. at 16 n.8. He asserts that the systems in place to protect the confidentiality of this information are "delicate" and "often inadequate," particularly in light of the "government's growing technological prowess." Id. at 16 & 22. These technological developments, he alleges, have caused increasing numbers of individuals to become concerned about the disclosure of private information. See, e.g., id. at 16 ("[T]he need to guard privacy rights against the fragile, imperfect protections of today's information systems is a matter of common knowledge and concern in today's complex, computer-connected society"); Reply Brief at 8 n.4 ("[T]he cavalier disclosure of names and addresses is increasingly under fire from many directions and sources. Indeed, people want to protect their privacy more and more, as evidenced by such modern 'inventions' as computer 'killfiles' and laws that permit phone customers to have their name and phone number deleted from telemarketing company databases."). Thus, appellant argues that it has "become ever more . . . vital" that Article I, Section 8 be construed broadly to encompass an individual's name and address. Id. at 22.

Appellant's subjective concerns about the inexorable advance of technology say little about this case. The government's "technological prowess" here consisted of police

picking up the low technology telephone and phoning appellant's bank. This hardly raises appellant's specter of "Big Brother."⁶ Moreover, even accepting as true appellant's averments that increasing numbers of people are concerned with governmental inroads upon their privacy, there is nothing in the record here to show that **this** appellant shared those concerns, let alone that he actually expected his bank not to disclose his mere name and address to law enforcement officials upon their request. As the Commonwealth notes, appellant certainly presented no evidence that he subjectively harbored such an expectation. Although appellant testified at the suppression hearing, he never claimed that he believed that his bank would keep his name and address private, nor did he present any other evidence suggesting a basis for any such expectation for Drovers Bank customers generally. Indeed, the bank manager, Robert Garrison, testified that the bank provided a list of its ATM card holders to independent mailing firms and that, to his knowledge, appellant never asked the bank to keep this information private. See N.T. 9/29/1997 at 18-19.

Moreover, appellant's conduct did not suggest that he ever actually regarded his name and address to be private information. An individual who wishes his identity as a bank customer to remain confidential might be highly circumspect in the use of an ATM card bearing both his name and card number. Such a person might be expected to use the card only in emergencies, or only at ATM machines, where others would be less likely to observe this "private" connecting information. But appellant was anything but cautious in the use of his ATM card. On the night of the rape, he entered a nearby pornography store monitored by video surveillance cameras and attempted to make a public purchase with the

⁶ George Orwell, 1984, at 4 (1949).

card. Appellant could have paid in cash or chosen some other payment option which did not reveal his identity or even his connection to a particular bank. But appellant did not do so.

The dissent asserts that, in executing a card-holder agreement which provided, *inter alia*, that his ATM card was "non-transferable," appellant exhibited a subjective expectation of privacy in the name and address information associated with his account. See Dissenting slip op. at 5. The actual text of the contract language adverted to by the dissent, however, provided: "I [appellant] agree that the money access card is non-transferable." N.T. 9/29/1997 at 17-18. Thus, by its express terms, the "non-transfer" restriction applied only to appellant; it in no way restricted the bank from disseminating information regarding appellant to third-parties. Moreover, the card-holder agreement also provided that the ATM card was the exclusive property of the bank, see id. at 17, which is inconsistent with any alleged belief on the part of appellant that the bank had assumed a duty to keep his name and address confidential.

Appellant further claims that the Commonwealth has waived the argument that he failed to present any evidence that he had a subjective expectation of privacy in the identifying information provided by the bank because it did not include it as an issue in its Statement of Matters Complained of on Appeal pursuant to Pa.R.A.P. 1925(b). We disagree. When the suppression court ruled against the Commonwealth, it appealed and claimed, among other things, that the police conduct in question did not implicate appellant's reasonable privacy expectations. There is nothing oblique or mysterious about such an argument; the two-part Katz test for assessing privacy expectations is well-settled in this Commonwealth. Moreover, the suggestion that the Commonwealth, the prevailing

party in the Superior Court, has waived a part of the governing, conjunctive constitutional test also runs afoul of our recent decision in Commonwealth v. Torres, 764 A.2d 532 (Pa. 2001). There, as here, the appellant prevailed upon a pre-trial motion seeking, *inter alia*, to suppress certain evidence under Article I, Section 8. The Commonwealth appealed, arguing that the appellant lacked standing to challenge a police search or, in the alternative, that the search warrant was supported by probable cause. The Superior Court reversed the order of the suppression court on the latter ground and the appellant appealed to this Court. Writing for the majority, Mr. Justice Nigro noted that "the Superior Court erred in concluding that the affidavit supplied the issuing authority with a substantial basis to conclude that there was probable cause [for the] search." Id. at 541. "However," he continued, "we affirm the decision of the Superior Court on an alternate basis -- that [appellant] has failed to demonstrate a subjective expectation of privacy in the premises searched." Id. (citing E.J. McAleer & Co. v. Iceland Products, Inc., 381 A.2d 441, 443 n.4 (Pa. 1977) for proposition that this Court may affirm lower court's decision on any proper basis regardless of specific basis on which lower court relied).

In any event, appellant's claim independently fails because we agree with the Commonwealth that any subjective expectation of privacy that appellant may have had in the name and address information is not an expectation which society would be willing to recognize as objectively reasonable in light of the realities of our modern age. Whether registering to vote, applying for a driver's license, applying for a job, opening a bank account, paying taxes, etc., it is all but impossible to live in our current society without repeated disclosure of one's name and address, both privately and publicly. There is nothing nefarious in such disclosures. An individual's name and address, by themselves, reveal nothing about one's personal, private affairs. Names and addresses are generally

available in telephone directories, property rolls, voter rolls, and other publications open to public inspection. In addition, it has become increasingly common for both the government and private companies to share or sell name and address information to unaffiliated third-parties. In fact, appellant's bank did just that:

Q: Now, Mr. Garrison, does your bank provide the names and addresses of your customers to anyone?

A: We have provided a listing of our ATM card holders to independent mailing firms.

The Court: I'm sorry?

The witness: Independent mailing firms, in order to send sales materials to the customer and also to sell other bank products.

N.T. 9/29/1997 at 18-19. In this day and age where people routinely disclose their names and addresses to all manner of public and private entities, this information often appears in government records, telephone directories and numerous other documents that are readily accessible to the public, and where customer lists are regularly sold to marketing firms and other businesses, an individual cannot reasonably expect that his identity and home address will remain secret -- especially where, as here, he takes no specific action to have his information treated differently and more privately.

We are further convinced of the correctness of our conclusion that no privacy expectation reposes in this information by the fact that the majority of courts to consider the question have agreed that a person's name and address is not information about which a person can have a reasonable expectation of privacy. For example, in State v. Chryst, 793 P.2d 538 (Alaska Ct. App. 1990), which was relied on by the Superior Court below, a local utility company responded to an informal police request by supplying the police with a list of all properties listed under the defendant's name. The defendant subsequently alleged that the disclosure of this information violated his privacy rights under the Alaska Constitution. Applying the same two-part Katz test used by this Court to determine whether Chryst's right to privacy was infringed, the Alaska Court of Appeals denied the claim, reasoning that:

[h]ad the police obtained Chryst's address from his driver's license application, or by checking public property records, there would be little claim that Chryst had a reasonable expectation of privacy from disclosure of his name and address from those sources even though Chryst was required to give that information to exercise his right to drive or own property. The information which is in dispute which [the utility company] gave the police was merely Chryst's name and address. It was information which was available because Chryst was a consumer of a public utility. Few people would regard the fact that they are consumers of the services of a public utility to be private information. We conclude that under the circumstances in this case, Chryst did not have a reasonable expectation of privacy which society is prepared to recognize in his name and address

Id. at 542 (footnote omitted). Similarly, the only "private" fact revealed by appellant's bank was that appellant was in fact the person who had a specific ATM account with them.

Appellant contends that Chryst is "not on point in any meaningful fashion" because the court "fail[ed] to analyze the issue under [its] state constitution" and thus the case "adds nothing to understanding the greater scope of protection accorded citizens' privacy rights by the Pennsylvania Constitution." Brief for Appellant at 20, 21. This is not so. Chryst's suppression claim was brought pursuant to the Alaska Constitution, and the claim was analyzed and decided under that state charter. See Chryst, 793 P.2d at 539 ("Chryst brought his motion to suppress under article 1, section 14 of the Alaska Constitution . . . and article 1, section 22 of the Alaska Constitution"); id. at 540 ("[T]he federal cases can be distinguished to some degree because the United States Constitution does not contain a special provision such as article 1, section 22 of the Alaska Constitution which specifically protects a right of privacy"); id. at 542 (Bryner, C.J., concurring) (noting that court was only construing "the reach of the Alaska Constitution's privacy clause"). In addition, appellant claims that this case is distinguishable because "the information in Chryst was drawn from public utility records, not the more secure records of bank accounts, where the expectation of privacy is greater because of the sensitive nature of the personal information contained

there." Brief for Appellant at 20. Yet, there is nothing in Chryst which suggests that the case turned on the source of the identifying information. Rather, it was the **nature** of the information disclosed -- the fact that individuals frequently "expose[] [their names and addresses] to the public," and that this mere identifying information, in and of itself, reveals nothing about "a person's activities, associations, and beliefs" -- which powered the Court's decision. Chryst, 793 P.2d at 541-42, quoting LaFave, supra. It is no more an invasion of privacy to disclose that a person is a bank customer than that he is a customer of a utility company.

Likewise, in Local 100, Service Employees' Int'l Union v. Forrest, 675 So.2d 1153 (La. Ct. App. 1996), a labor union filed a request with the Louisiana Department of Health and Hospitals (DHH) seeking a list of the names of all certified nurse's aides, along with their telephone numbers, addresses and places of employment. DHH refused to provide the information on the basis that the nurse's aides had an overriding privacy interest in the information under the Louisiana Constitution. Employing the two-pronged Katz test, the Louisiana Court of Appeals concluded that the employees did not have a reasonable expectation of privacy in their identities or addresses. Id. at 1157.

The Michigan Supreme Court also declined to find a right of privacy in one's name and address in Tobin v. Michigan Civil Service Comm'n, 331 N.W.2d 184 (Mich. 1982). In that case, five classified civil service employees of the State of Michigan filed a class action seeking to enjoin the state from releasing to several labor organizations a list of names and addresses of all classified civil service employees. Noting that "[n]ames and addresses are not ordinarily personal, intimate, or embarrassing pieces of information [and that] the supposed right to keep such information secret is at best riddled with exceptions[.]" the court held that disclosure of this information would not violate the plaintiffs' right of privacy under the Michigan or federal constitutions. Id. at 189-91.

Similarly, in Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995), the plaintiffs alleged that American Express's practice of renting lists of its cardholders' names and addresses, which categorized them according to their spending habits, constituted an invasion of their privacy. Recognizing that the disclosure of an individual's name and address does not present the same type of privacy concerns as the disclosure of information concerning private financial dealings, the Appellate Court of Illinois denied the claim:

Defendants rent names and addresses after they create a list of cardholders who have certain shopping tendencies; they are not disclosing financial information about particular cardholders. These lists are being used solely for the purpose of determining what type of advertising should be sent to whom. . . . Thus, we hold that the alleged actions here do not constitute an unreasonable intrusion into the seclusion of another.

Id. at 1355.

In State v. Smith, 367 N.W.2d 497 (Minn. 1985), the Supreme Court of Minnesota held that the disclosure of the defendant's current address by welfare officials did not violate his federal constitutional rights. Smith alleged, *inter alia*, that the disclosure violated his Fourth Amendment rights and he sought to suppress evidence linking him to a murder which was seized, claiming it to be the tainted fruit of this illegally obtained information. The court rejected the claim, noting that "a murderer's expectation that welfare officials will not provide his address to police officers who have probable cause to arrest him is not the sort of expectation that society considers reasonable under the Fourth Amendment or under any other provision of the Federal Constitution." Id. at 505.

The Supreme Court of Connecticut has reached a similar conclusion. In Town of West Hartford v. Freedom of Info. Comm'n, 588 A.2d 1368 (Conn. 1991), a firefighters' association requested the names and addresses of all retired residents of the Town of

West Hartford under the state's freedom of information act. The town provided a list of the names but denied the request for the addresses. The court observed that:

[i]t cannot seriously be questioned . . . that, as a general rule, addresses are publicly available. A person's address is known by his neighbors and is ordinarily published in public telephone and municipal directories. Absent specific requests for nondisclosure, mail order houses disclose addresses to those seeking such information for advertising purposes.

Id. at 1371-72. Accordingly, the court reversed the trial court's conclusion that disclosure of the retirees' addresses would per se constitute an invasion of personal privacy.

The two decisions of our sister jurisdictions primarily relied upon by appellant and the dissent, People v. Chapman, 679 P.2d 62 (Cal. 1984), and State v. Butterworth, 737 P.2d 1297 (Wash. Ct. App. 1987), are decidedly inapposite. In Chapman, the police obtained an unpublished telephone number from an informant who claimed that she had used the number to place illegal bets. Acting without a warrant, the police contacted the telephone company and obtained the name and address corresponding to the unpublished number, which were then used to obtain a search warrant. The warrant was executed and evidence of illegal betting was seized. The California Supreme Court held that, under the California Constitution, the defendant had a reasonable expectation of privacy in the unpublished listing and that such information may not be released without a warrant. In so holding, the court found persuasive the fact that the defendant had specifically requested that her identity be kept confidential and had paid an extra fee to the telephone company to protect her anonymity:

[B]y affirmatively requesting and paying an extra service charge to the telephone company to keep her unlisted information confidential, [the defendant] took specific steps to ensure greater privacy than that afforded other telephone customers. Surely those steps entitle [the defendant] to as great a degree of privacy as this court has extended to the customers in Burrows and [People v.] Blair], 602 P.2d 738 (Cal.

1979) (warrantless disclosure of telephone toll records violates California Constitution)].

Id. at 68. Indeed, the court suggested that if Chapman had not specifically requested confidentiality, she would not have had a reasonable expectation of privacy in the name and address information disclosed to the police, commenting that "[t]he fact that many customers do not seek to keep their identities or telephone numbers private does not in any way diminish the privacy rights **of those who do.**" Id. (emphasis added).

In Butterworth, the police received information from a confidential informant that the defendant was operating a marijuana "grow operation" out of his house, and they contacted the regional telephone company in an effort to ascertain the location of the residence. The telephone company indicated that it had a listing for the defendant, but that the listing was unpublished. The police then obtained the defendant's address and telephone number by making a written request to the telephone company's security department. When the police proceeded to the defendant's address, they smelled a strong odor of growing marijuana. This information, together with the anonymous tip, formed the basis for the issuance and execution of a search warrant, which in turn led to the seizure of several pounds of marijuana. In concluding that the defendant had a reasonable expectation of privacy in his unpublished telephone listing, and that the police violated his privacy rights under the Washington Constitution in obtaining this information without a warrant, the Washington Court of Appeals, like the Chapman court, emphasized that the defendant had "specifically requested privacy regarding his address and telephone number in asking for an unpublished listing. . . ." Id. at 1300; see also State v. Faydo, 846 P.2d 539, 541 (Wash. Ct. App. 1993) (declining to extend Butterworth to disclosure of name associated with

published telephone number where defendant made no request to keep his identity confidential).

Thus, both Chapman and Butterworth pivoted, to a significant extent, on the fact that in each case the defendant took specific action to protect his identity by requesting an unpublished telephone number. The banking equivalent of an unlisted telephone number would perhaps be the proverbial secret Swiss bank account or other similar banking arrangement, where the depositor has taken specific steps to conceal his identity. But it is not the generic account opened and maintained by appellant *sub judice*. Here, there is no evidence that appellant requested that his name and address be kept confidential, paid an additional fee to the bank to ensure that this identifying information was not disclosed, or took any other action to protect his identity merely as the bank's customer. Thus, even if we were to find these two decisions of our sister jurisdictions persuasive under the Pennsylvania Constitution, they would not support appellant's claim here. We hold, consistently with the realities of our modern, consumer age and the experience of other courts, that appellant does not have an expectation of privacy in his name and address that society is willing to recognize as reasonable and legitimate.

In conclusion, DeJohn does not support the proposition that the police request for appellant's name and address implicated appellant's privacy rights under Article I, Section 8, and we hold that a novel expansion of our search and seizure jurisprudence to encompass such a request is not warranted.⁷ Accordingly, we affirm the well-reasoned decision of the Superior Court below and remand the case for trial.

⁷ The dissent expresses concern that, in light of the Court's holding today that the police conduct here was constitutionally permissible, there will be "nothing to stop law (continued...)"

Mr. Justice Nigro files a dissenting opinion in which Mr. Chief Justice Cappy joins.

(...continued)

enforcement officers from obtaining lists of ATM account numbers utilized at select targeted establishments and then telephoning the respective banks to compile a full list of names and addresses of citizens frequenting those establishments." Dissenting slip op. at 4-5. This assertion misses the mark. Strictly speaking, **nothing** that this Court does in a case involving a suppression issue **prevents** police from doing anything, such as making telephone calls; the question is one of whether to provide a trial remedy. On that question, the obvious answer to the dissent's exaggerated fear is that the probable cause requirement, for one, stands in the way of admitting evidence that police seized for no reason other than to compile a list of citizens frequenting a "targeted establishment." In this case, as the dissent concedes, see id. at 4 ("[T]here was nothing to prevent the police in this case from obtaining a warrant for bank records showing the name and address that corresponded to the ATM card number at issue"), there is no question that police had probable cause to believe that the person whose identity they were seeking to ascertain was the suspected rapist. The other "protection" against such requests is the bank's authority to say "no." That is a private matter a customer should take up with his bank; it does not trigger constitutional concerns.