

COMMONWEALTH OF PENNSYLVANIA,	:	IN THE SUPERIOR COURT OF
	:	PENNSYLVANIA
Appellant	:	
	:	
v.	:	No. 494 Philadelphia 1998
	:	
DAVID DUNCAN	:	

Appeal from the Order Entered January 5, 1998,
in the Court of Common Pleas of Philadelphia County
Criminal Division, No. 9704-0280 1/1

BEFORE: FORD ELLIOTT, STEVENS, AND ORIE MELVIN, JJ.

*****Petition for Reargument Filed 4/14/2000*****

OPINION BY FORD ELLIOTT, J.: Filed: April 4, 2000

*****Petition for Reargument Denied 6/6/2000*****

¶ 1 The Commonwealth appeals from the trial court’s order granting appellee David Duncan’s motion to suppress.¹ We reverse and remand.

¶ 2 The relevant facts as found by the trial court and supported by the record are as follows. At approximately 6:00 p.m. on November 10, 1996, a man approached the victim near 20th Street and John F. Kennedy Boulevard in the city of Philadelphia and asked her if she was “working.” She said no, and continued walking. The man again approached her, this time claiming to have a gun and threatening to kill her if she did not do as she was told.

¹ “[T]he Commonwealth’s appeal of a suppression order is proper as an appeal from a final order when the Commonwealth certifies in good faith that the suppression order terminates or substantially handicaps its prosecution.” *Commonwealth v. Dugger*, 506 Pa. 537, 546-547, 486 A.2d 382, 386 (1985); 42 Pa.C.S.A. § 5105(a). This certification must be filed with the Commonwealth’s Notice of Appeal. Pa.R.App.P. 311(d), 940(e). The Commonwealth has properly filed its *Dugger* statement.

The man escorted her to a closet beneath the Conrail train tracks where he raped her and stole her money.

¶ 3 During the incident, the victim had an opportunity to see her attacker as they walked for approximately 15 to 20 minutes. She described him 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. The police surveyed area pornography shops, and a cashier from Elgee's Novelty reported that a man matching the victim's description had been in the store near the time of the rape. The cashier further reported that the alleged attacker attempted to make a purchase using a money access bank card, but the card was declined. The cashier provided the police with a list of credit card transactions for that day which identified the bank and account numbers for two cards that were declined. In addition, the police viewed the store's surveillance videotape, which showed a man in an Eagles jacket attempting to make a purchase.

¶ 4 After eliminating one suspect whose bank card transaction was declined, Officer Carl Latorre telephoned Robert Garrison, the manager of Drivers and Mechanics Bank in York, Pennsylvania and requested, without a warrant, the name and address of the owner of the other declined bank card. Mr. Garrison complied with the request, identifying appellee David Duncan whose address was in York County.

¶ 5 The police then requested the York County authorities to obtain and execute a search warrant for appellee's blood, bodily fluids, and hair. York County also provided Officer Latorre with an eight-photo array, which included a photograph of appellee. The photo array was shown to the victim but she failed to identify appellee. Appellee was arrested on March 14, 1997. On March 20, 1997, the prosecutor, who had been told by the victim that she felt she could identify her attacker if she saw him in person, requested a lineup. The prosecutor did not inform defense counsel or the municipal court judge that the victim had failed to identify appellee in a photo array. A lineup was held at which the victim identified appellee as her attacker.

¶ 6 Appellee filed an omnibus motion to suppress in relevant part the identifying information obtained from the bank, the blood, bodily fluids and hair evidence, the lineup identification, and the victim's in-court identification of appellee. At a hearing on the motion, the Commonwealth presented testimony from Officer Latorre, the bank manager, and the victim. The defense presented testimony from appellee and stipulated testimony from appellee's prior counsel regarding the prosecutor's failure to inform of the photo array non-identification. Appellee admitted that he was in Philadelphia all day during the day of the attack wearing a dark green Eagles jacket with a new logo purchased that day.

¶ 7 The trial court found that the warrantless request for appellee's name and address violated appellee's constitutional right to privacy in his bank records under the Pennsylvania Constitution and our supreme court's decision in *Commonwealth v. DeJohn*, 486 Pa. 32, 403 A.2d 1283 (1979), *cert. denied*, 444 U.S. 1032 (1980). (Trial court opinion, 7/21/98 at 5.) The trial court therefore suppressed appellee's name and address obtained from the bank. (*Id.*) The blood, bodily fluid and hair evidence, and the lineup identification were suppressed as tainted fruit of the initial illegal search of appellee's bank records. (*Id.*) In addition, the trial court concluded that the failure to disclose the photographic identification evidence was prosecutorial misconduct and that the victim's identification of appellee at the lineup might have been influenced by her memory of seeing appellee's photo. (*Id.*) Finally, the victim's in-court identification was not suppressed because the trial court found that she had an independent basis for the identification due to her ample opportunity to observe her attacker during the incident and her detailed description of the defendant. (*Id.* at 6.)

¶ 8 The Commonwealth raises the following issues on appeal:

1. Where a police officer was investigating a rape in which someone who fit the description of the rapist used an ATM card in a store near the rape scene, did the officer violate defendant's right to privacy by asking his bank for his name and address?
 - 1(a). Did the bank have apparent authority to allow the police access to defendant's name and address

consistent with its ownership of the ATM card, and pursuant to an agreement with the bank signed by defendant?

2. Where the police obtained a warrant to obtain blood and hair samples from defendant, did the lower court err in ruling that the manner in which police discovered defendant's identity, which cannot be suppressed, required suppression of blood tests?
3. Did the lower court err in suppressing a lineup identification where there was no claim and no finding that the lineup was suggestive, the Commonwealth had no duty to inform defendant that the victim had previously failed to make a photographic identification, and this failure in a nonexistent duty did not make the lineup any less reliable?

Commonwealth brief at 2.²

¶ 9 On review of a grant of a motion to suppress, we consider only the evidence of the defendant's witnesses and so much of the evidence of the Commonwealth that remains uncontradicted. *Commonwealth v. Prosek*, 700 A.2d 1305, 1307 (Pa.Super. 1997). "When the factual findings of the suppression court are supported by the evidence, we may reverse only if

² Although appellee has not cross-appealed, he attempts to assert issues not raised by the Commonwealth. Briefly, appellee argues that the Commonwealth lacked probable cause at virtually every stage of the investigation, and that "ongoing" constitutional violations require suppression of the physical and lineup evidence. (Appellee's brief at 2.) We find these issues meritless. The trial court found that there was probable cause. (Notes of testimony, 9/29/97 at 90-91.) We also find that the relevant search warrants contain sufficient probable cause. Appellee's "ongoing violations" argument is nothing more than a litany of allegations of prosecutor wrongdoing. We note that we address the relevant allegations of wrongdoing as set forth in appellee's properly asserted counter issues, and otherwise decline to address appellee's remaining allegations.

there is an error in the legal conclusions drawn from those factual findings.” *Commonwealth v. Farrell*, 672 A.2d 324, 325 (Pa.Super. 1996).

¶ 10 The trial court viewed the Commonwealth’s first issue in the instant case as identical to the issue in *DeJohn*, framing it as “whether the defendant had a privacy interest in the bank records and whether the Commonwealth has violated that interest.” (Trial court opinion, 7/21/98 at 4.) According to the trial court, *DeJohn* “makes no distinction whether the [warrantless] inquiry [into the bank records] is to discover criminal motive or the suspect’s identity.” (*Id.*) Thus, to the trial court the fact that the police only sought appellee’s name and address and not his financial data was an irrelevant distinction under *DeJohn*. The trial court therefore found *DeJohn* to control the instant issue and suppressed appellee’s name and address because the police obtained this information without a valid search warrant.

¶ 11 On appeal, however, both the Commonwealth and appellee address the issue of whether a bank customer has a constitutionally protected privacy interest in his name and address as connected with his bank records. The Commonwealth argues that because it did not seek appellee’s financial information but only identification information, *DeJohn* is inapplicable. Thus, the Commonwealth argues that appellee does not have a constitutionally protected privacy interest in his name and address. (Commonwealth brief at 13.)

¶ 12 Appellee asserts, however, that his expectation of privacy was “not just [in] his name and address, but [in] his privacy in the connection of his name and address to a particular account number.” (Appellee’s brief at 14.)³ Appellee therefore argues that the ruling of *DeJohn* applies because a customer’s reasonable expectation of privacy in his bank records must encompass the customer’s name and address. (*Id.* at 12.) In support of his argument, appellee urges us to follow California case law as persuasive reasoning that one has a constitutional right to privacy in one’s name and address. (*Id.* at 12-14, citing *People v. Chapman*, 36 Cal.3d 98, 201 Cal. Rptr. 268, 679 P.2d 62 (Cal. 1984).) Finally, appellee argues that the discovery of his name and address is “both revealing and compelling” such that it implicates a right to privacy similar to that afforded financial information or a record of telephone numbers dialed. (Appellee’s brief at 14-15, citing *Commonwealth v. Beauford*, 475 A.2d 783 (Pa.Super. 1984) (following *DeJohn* in rejecting federal law and finding constitutionally protected right to privacy under Article I, § 8 of the Pennsylvania Constitution in pen register of telephone numbers).) We disagree and conclude that the name and address information discovered by the police in the instant matter is substantively different from information afforded constitutional protection.

³ We note that appellee concedes that in this case he had no right to privacy to his account number. (Notes of testimony, 9/29/97 at 94.)

¶ 13 This case presents an issue of first impression under Article I, Section 8 of the Pennsylvania Constitution, which 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 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.

Pennsylvania recognizes that it “has the constitutional power to grant individual rights, including the right to be free from unreasonable searches and seizures, more zealously than the federal government does under the United States Constitution.” *Beauford*, 475 A.2d at 788 (citations omitted). “[T]oday the constitutional prohibition against unreasonable searches and seizures extends beyond the home to protect the individual against unwarranted government intrusions into any area where the individual may harbor a reasonable expectation of privacy.” *Id.* at 787, citing *Katz v. United States*, 389 U.S. 347 (1967) (other citations omitted). In *DeJohn*, our supreme court made explicit that “the right to be free from unreasonable searches and seizures contained in Article [I], Section 8 of the Pennsylvania Constitution is tied into the implicit right to privacy in this Commonwealth.” *DeJohn, supra* at 49, 403 A.2d at 1291.

¶ 14 Our Constitution protects, however, only “those zones where one has a reasonable expectation of privacy.” *Commonwealth v. Blystone*, 519 Pa. 450, 463, 549 A.2d 81, 87 (1988), *aff’d on other grounds sub nom.*

Blystone v. Pennsylvania, 494 U.S. 299 (1990), citing *DeJohn, supra* at 44, 403 A.2d at 1289. “To determine whether one’s activities fall within the right of privacy, we must examine: first, whether the person exhibited an expectation of privacy; and second whether that expectation is one that society is prepared to recognize as reasonable.” *Commonwealth v. Brion*, 539 Pa. 256, 260, 652 A.2d 287, 288-289 (1994), quoting *Blystone, supra* at 463, 549 A.2d at 87. “We consider the totality of the circumstances and carefully weigh the societal interests involved when determining the legitimacy of such an expectation.” *Commonwealth v. Johnson*, 556 Pa. 216, ___, 727 A.2d 1089, 1098 (1999), *cert. denied*, 2000 WL 197675 (U.S. Feb. 22, 2000).

¶ 15 In *DeJohn*, our supreme court held that under the Pennsylvania Constitution, bank customers have a reasonable expectation of privacy in “records pertaining to their affairs kept at the bank.” *DeJohn, supra* at 49, 403 A.2d at 1291.⁴ In reaching its conclusion, *DeJohn* expressly declined to follow federal precedent holding that a bank customer does not have a legitimate expectation of privacy in the information contained in bank records under the United States Constitution. *Id.* at 44, 403 A.2d at 1289 (rejecting *United States v. Miller*, 425 U.S. 435 (1976) (no expectation of

⁴ Specifically, in *DeJohn*, the police sought from the bank, pursuant to two invalid subpoenas, “copies of all information pertaining to accounts, or application for account,” and “all original records pertaining to personal cash reserve account application, and original new account card.” *DeJohn, supra* at 40, 403 A.2d at 1287.

privacy in bank records under Fourth Amendment)). Thus, Pennsylvania “extend[s] more privacy protection to banking records under article 1, § 8, than the United States Supreme Court provides under the federal constitution.” *Beauford*, 475 A.2d at 788, citing *DeJohn, supra*.

¶ 16 In *DeJohn*, our supreme court found the California Supreme Court’s analysis of the same issue to be persuasive. *DeJohn, supra* at 45-48, 403 A.2d at 1289-1291, citing *Burrows v. Superior Court of San Bernardino County*, 13 Cal.3d 238, 118 Cal. Rptr. 166, 529 P.2d 590 (Cal. 1974). Quoting extensively from *Burrows*, our supreme court adopted its reasoning. *Id.*

¶ 17 Following *Burrows*, our supreme court reasoned that the disclosure of “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.” *DeJohn, supra* at 45, 403 A.2d at 1289 (citation and quotation omitted). Furthermore, divulging one’s financial affairs to a bank “reveals many aspects of [one’s] personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography.” *Id.* The *DeJohn* court also noted that “[t]he disclosure by the depositor to the bank is made for the limited purpose of facilitating the conduct of his financial affairs; it seems evident that his expectation of privacy is not diminished by the bank’s retention of a record of such disclosures.” *Id.* at 48, 403 A.2d at 1291 (citation and quotation omitted).

¶ 18 Like Pennsylvania, several of our sister states also provide for more extensive protection of their citizens' privacy rights under their state constitutions than the United States Supreme Court does under the Federal Constitution. *See, e.g., State v. Glass*, 583 P.2d 872 (Alaska 1978); *People v. Burrows, supra*; *Charnes v. DiGiacomo*, 200 Colo. 94, 612 P.2d 1117 (Colo. 1980); *State v. Thompson*, 114 Idaho 746, 760 P.2d 1162 (Idaho 1988); and *State v. Myrick*, 102 Wash.2d 506, 688 P.2d 151 (Wash. 1984). Our research has revealed that no other state has addressed the precise issue before us. However, of the states that afford more privacy protection under their constitutions, several have determined the extent of a person's right to privacy under their state constitution with respect to name and address information of customers of telephone companies and utility companies. *Compare Chapman, supra* (reasonable expectation of privacy in name and address connected with unlisted telephone number), and *State v. Butterworth*, 48 Wash. App. 152, 737 P.2d 1297 (Wash. Ct. App. 1987) (same), with *D'Antonio v. State*, 837 P.2d 727 (Alaska Ct. App. 1992) (no reasonable expectation of privacy in identifying information connected with private mail services), *State v. Chryst*, 793 P.2d 538 (Alaska Ct. App. 1990) (no reasonable expectation of privacy in name and address connected to utility company), and *State v. Faydo*, 68 Wash. App. 621, 846 P.2d 539 (Wash. Ct. App. 1993) (no reasonable expectation of privacy in name and address connected with listed telephone number).

¶ 19 Contrary to appellee's contention, we find that *Chapman* is distinguishable from the present case. In *Chapman*, a police officer, acting without a warrant, asked for and received the name and address of the subscriber to an unlisted number. The *Chapman* court held that under the California Constitution, a telephone company subscriber has a reasonable expectation of privacy in her name and address associated with her unlisted telephone number. In support of its ruling, the *Chapman* court reasoned that "by 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." *Chapman*, 36 Cal.3d at ___, 201 Cal. Rptr. at ___, 679 P.2d at 68. Here, appellee did not request privacy with respect to the fact that he is a bank customer, nor did he pay an extra fee to ensure confidentiality with respect to his name and address. Thus, we are not asked to determine whether one has a higher expectation of privacy in name and address information when one affirmatively obtains an agreement for confidentiality with respect to his or her identification information.⁵

⁵ Likewise, the *Butterworth* court noted that the defendant "specifically requested privacy regarding his address and telephone number in asking for an unpublished listing." *Butterworth*, 48 Wash. App. at ___, 737 P.2d at 1300. Moreover, in *Faydo, supra*, the court distinguished *Butterworth* in holding that no constitutional violation occurred when police obtained defendant's name and address by requesting the same from the telephone company without a warrant. *Faydo*, 68 Wash. App. at ___, 846 P.2d at 625. The *Faydo* defendant did not request that his identity be kept confidential. *Id.*

¶ 20 A more analogous situation is presented in *State v. Chryst, supra*, in which the Court of Appeals of Alaska concluded that an electric utility customer does not have a reasonable expectation of privacy in his address information given to a company for the purpose of obtaining service. The Alaska court noted that “a person’s name and address, *by themselves*, do not constitute information about which a person can have a reasonable expectation of privacy which society is willing to recognize.” *Chryst*, 793 P.2d at 543 (emphasis added). The *Chryst* court, in explaining that one does not have a reasonable expectation of privacy, stated as follows:

Had 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.

Id. 793 P.2d at 542.

¶ 21 The *Chryst* court also relied on authority from Professor LaFave who, while criticizing the United States Supreme Court’s decision in *Miller*, acknowledged that not all of a person’s information implicates the right to privacy under the Fourth Amendment.

'Admittedly it cannot be said that all information about a person is private in the Fourth Amendment sense. **Katz** instructs that "[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 fits 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. [(So too, there is no legitimate expectation of privacy as to certain other information acquired by police examination of the government's own files.)] But bank records are another matter, for unquestionably they "can reveal much about a person's activities, associations, and beliefs."

Chryst, 793 P.2d at 541-542, quoting W. LaFave, Search and Seizure § 2.7(c), at 512-513 (2d ed. 1987) (footnotes omitted, ellipsis in original) (brackets added to include update from W. LaFave, *supra*, (3d ed. 1996)). Finally, in his concurring opinion in **Chryst**, Chief Judge Bryner noted that both **Chapman** and **Butterworth**

involved situations in which the customer's address was associated with an unlisted telephone number. In both cases, the unlisted number was the core information found to be protected by the right to privacy, and the customer's address was protected as a consequence of its relationship to the protected information. Neither case purports to hold that a person's address is in and of itself private information whose disclosure is constitutionally protected

Chryst, 793 P.2d at 543, citing **Chapman**, *supra* and **Butterworth**, *supra*. See also **D'Antorio v. State**, *supra* (finding **Chryst** controlled

issue of warrantless request of defendant's private mail services for the name of the person who opened the mailbox, the time it was opened, and the directions for forwarding the mail).

¶ 22 Also helpful to our analysis of the instant issue is the reasoning of state court cases that have addressed the extent of state constitutional privacy protection afforded a customer's raw data generated by a utility company. *See Samson v. State*, 919 P.2d 171 (Alaska Ct. App. 1996) (no reasonable expectation of privacy in power consumption utility records); *People v. Dunkin*, 888 P.2d 305 (Colo. Ct. App. 1994), *cert. denied sub nom. Smith v. Colorado*, 515 U.S. 1105 (1995) (same); and *State v. Kluss*, 867 P.2d 247 (Idaho Ct. App. 1993) (same). The above cases highlight the fundamental difference between constitutionally protected bank record and telephone record information and non-protected information. In particular, the *Kluss* court noted that power usage information

does not provide any intimate details of Kluss's life, identify his friends or political and business associates, nor does it provide or complete a 'virtual current biography.' The power records, unlike telephone or bank records, do not reveal discrete information about Kluss's activities.

Kluss, 125 Idaho at ____, 867 P.2d at 254. *See also Samson*, 919 P.2d at 174, and *Dunkin*, 888 P.2d at 307. The *Kluss* court also distinguished *Chapman* by noting "that the telephone subscriber [in *Chapman*]. . . had paid an extra fee to the telephone company for the unlisted number."

Kluss, 125 Idaho at ____, 867 P.2d at 253.

¶ 23 Finally, Judge Mannheim, in his concurring opinion in *Samson*, further noted that “gross electricity usage reveal[s] no details of the activities that consumed the electricity,” whereas “[b]ank records list the details of a customer’s financial dealings – names of debtors, creditors, and most others with whom the customer does business.” *Samson*, 919 P.2d at 173 (Mannheimer, J. concurring, joined by Bryner, C.J.); *see also DeJohn, supra* at 45, 403 A.2d at 1289.⁶

¶ 24 Our review of the case law from Pennsylvania and our sister states persuades us to conclude 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. We conclude that a constitutionally recognized right to privacy in one’s information in bank and telephone records is based in the content of that information and in the specific aspects of a person’s private life that might be revealed by divulging that information. The ‘virtual current biography’ revealed by public disclosure of information deserving constitutional protection consists of the unique, perhaps controversial or

⁶ We decline to comment on whether Pennsylvania would recognize a right to privacy in its citizens’ power usage records, noting only that such information is substantively different from the identification information in the present case. In addition, our supreme court in *Commonwealth v. Gindlesperger*, ___ Pa. ___, 743 A.2d 898 (1999), found that one has a reasonable expectation of privacy in the heat escaping from one’s home such that the warrantless use of an infrared thermal imaging device of a private residence violates the Fourth Amendment of the United States Constitution. *See also Matter of Maxfield*, 133 Wash.2d 332, 945 P.2d 196 (Wash. 1997) (holding defendant had protected privacy interest in electric consumption records under state constitution).

unpopular, essence of one's personality rather than merely identifying individuals, where they live, and their telephone number. Thus, the case law instructs us that private information protected under our state constitution is properly characterized, in part, as revealing many aspects of one's personal affairs, activities, beliefs, opinions, habits, and associations; moreover, the release of such private information may undermine one's political liberty, including the right to associate, to express one's views, and to think in freedom. *See e.g., DeJohn, supra*, and *Beauford, supra*. We therefore conclude "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." *Chryst*, 793 P.2d at 542 (agreeing with LaFave, *supra*).

¶ 25 In the instant case, the police discovered the name and address of a person they suspected of committing the crime, thereby allowing the police to secure a search warrant for appellee's blood, bodily fluids, and hair. To appellee, that discovery is both revealing and compelling, and violated his right to privacy, because it completed his "current biography." (Appellee's brief at 14-15.) However, we are unpersuaded that appellee has a right to privacy grounded solely in his desire to protect himself from being identified as the perpetrator of a crime. While appellee may have expected that his identity as a suspect would remain private, his expectation is not one that society is prepared to recognize as reasonable. We recognize that there

may be a situation where a person does have a reasonable expectation of privacy in one's name and address that would prevent the police from obtaining the information without a warrant, and thereby protect a person's identity as a suspect. However, the burden is on the person asserting the right of privacy to demonstrate that the name and address information is constitutionally protected apart from one's desire to avoid being identified as a perpetrator of a crime. Appellee here has failed to demonstrate that his right to keep the fact that he is a customer of the bank private is of constitutional significance.⁷

¶ 26 Based on the character of the above components that contribute to a person's virtual current biography, we fail to see how the discovery of appellee's name and address, disclosed by his bank, reveal (or complete) a virtual current biography of appellee. We therefore hold that a customer who has not requested confidentiality does not have a reasonable expectation of privacy in his name and address as a customer of a bank. In light of our holding, we find that the trial court erred in concluding that

⁷ We also note that it is unlikely, absent an agreement to the contrary, that one has a right to privacy in the fact that one is a customer of a bank. Indeed, the case law reveals that it is not the fact of actually being a customer by itself that is constitutionally significant. Pennsylvania's departure from federal law is rooted in the realistic observation that for most, if not all, of our citizens, active participation in contemporary society requires that one maintain a bank account (or telephone access). *See DeJohn, supra, Beauford, supra.* Implicit in this observation is the recognition that a citizen is most likely a bank (or telephone company) customer. Thus, our cases have concerned the underlying content of selected private information that, as a practical necessity, a citizen must release in order to participate in modern society.

DeJohn controls, and therefore that appellee's constitutional right to privacy was violated, and in suppressing the discovery of his name and address.

¶ 27 Based on our resolution of this issue, we need not address the Commonwealth's argument that appellee's name and address are not protected because the bank divulges such information to an independent mailing firm in order to market other bank products to its customers.⁸ We note that in addressing this argument, appellee argues that the disclosure by the bank for marketing purposes is akin to the limited exposure that occurs when a customer negotiates a check and exposes information to third parties. (Appellee's brief at 13-14, n.5 (arguing that mailing firm is acting as agent of bank).) The *DeJohn* court held that such limited disclosure does not defeat a customer's expectation of privacy in his *financial* records. *DeJohn, supra* at 46-47, 403 A.2d at 1290-1291. Appellee, however, again fails to explore the substantive differences between financial information and identification information, and merely suggests that the nature of the information obtained is not constitutionally significant. (Appellee's brief at 14.) In addition, we note that the use by the bank of name and address information to solicit its customers is distinguishable from

⁸ We also need not address the Commonwealth's sub-issue that appellee's name and address is not confidential because appellee had signed an agreement stating that the bank card was the exclusive property of the bank. We note, however, there is no record evidence indicating that the agreement properly concerns the privacy of the cardholder's name and address, but only purports to establish that the bank holds property rights in the card itself.

the use by the bank of customer information to conduct its primary business purpose as a bank.⁹

¶ 28 Because appellee's name and address were validly obtained, we also find that the trial court erred in suppressing appellee's blood, bodily fluids, and hair samples as tainted fruit of an illegal search.

¶ 29 Finally, we address the Commonwealth's claim that the trial court erred in suppressing the victim's identification of appellee at a lineup. The trial court ultimately suppressed the lineup evidence based on its ruling that the lineup was a fruit of the initial illegal search to obtain appellee's name and address. (Trial court opinion, 7/21/98 at 6.) Because we find no constitutional violation, the lineup evidence cannot be suppressed because of an illegal search. However, the trial court also "considered numerous factors in reaching its decision that the initial taint extended to the line-up identification" (*Id.* at 5.) Specifically, the trial court explained as follows:

A major factor was the fact that the Commonwealth continuously failed to disclose the complainant's failure to make a photo identification. This was prosecutorial misconduct which denied the defense a fair opportunity to avoid a suggestive line-up identification. Because the witness had seen [appellee's] photo, the court felt she may have been influenced by the memory of the photo in making a line-up identification.

⁹ We also recognize that "in this day and age in which private businesses routinely sell customer lists to other businesses, it [may be] unreasonable to believe a customer's name[, absent an agreement to the contrary] . . . will be kept private." *Faydo*, 846 P.2d 541.

Moreover, the Commonwealth actions prohibited a meaningful hearing before the Municipal Court Judge on the issue of whether or not a line-up was appropriate.

Id.

¶ 30 We disagree with the trial court's finding that the nondisclosure of the photo array identification procedure amounted to prosecutorial misconduct. In *Commonwealth v. Floyd*, 508 Pa. 393, 498 A.2d 816 (1985), relied upon by the trial court, the Commonwealth failed to disclose to the defense that a witness identified the defendant from a photo array viewed before trial. The defense had properly requested discovery, but the Commonwealth did not "disclose" the prior identification until it introduced the evidence at trial in response to the witness' cross-examination testimony that he had never identified the defendant. The supreme court found that the Commonwealth's conduct violated Rule of Criminal Procedure 305(B)(1)(d), which requires that the Commonwealth disclose "the circumstances and results of any identification of the defendant." Pa.R.Crim.Proc. 305(B)(1)(d), 42 Pa.C.S.A. The supreme court then stated that the remedy for failing to disclose the required information – the grant of a new trial – is required "unless [the nondisclosure] can be shown to have been harmless beyond a reasonable doubt." *Id.*, *supra* at 397, 498 A.2d at 818. In *Floyd*, the non-disclosure was found prejudicial and a new trial was granted.

¶ 31 The instant case is distinguishable. Here, at the time the prosecutor requested a lineup, defense counsel had not requested any discovery pursuant to Rule 305(B)(1)(d). Neither the trial court nor appellee has cited any authority to support the position that the Commonwealth was required to disclose the pre-arrest identification procedure before discovery had been requested. In fact, the trial court explained its position, in part, by opining that the Commonwealth should have “just disclose[d] [the information regarding the photo lineup]. There is no rule that requires you to disclose it at that point, no rule of procedure. However in complete candor to the Court I believe that is the best policy.” (Notes of testimony, 12/11/97 at 13.)¹⁰ Significantly, and in contrast to *Floyd*, the Commonwealth here did disclose the non-identification after pre-trial discovery had begun. Under the facts of this case, we therefore find that the trial court erred in concluding that the non-disclosure was prosecutorial misconduct.¹¹

¹⁰ We agree that the best policy is candor to the court. However, there is no record evidence that the prosecutor intentionally concealed or chose not to disclose the photo array procedure or otherwise exhibited bad faith. The record here is simply devoid of any inquiry by defense counsel or the trial court into why the information was not disclosed when the lineup was requested.

¹¹ Appellee relies on *Commonwealth v. Melson*, 556 A.2d 836 (Pa.Super. 1989), *appeal denied*, 525 Pa. 579, 575 A.2d 111 (1990), in which the prosecutor improperly lured the defendant into a suggestive one-on-one identification by compelling his attendance at a co-defendant’s sentencing where a witness identified him. Apparently, appellee argues that the present case is analogous in that the prosecutor here “lured” appellee into a suggestive lineup by not informing defense counsel of the prior non-identification. There is no record evidence to support appellee’s contention. We fail to see how *Melson* is applicable to the instant case.

¶ 32 At the suppression hearing, defense counsel had the opportunity to assert a claim of improper identification. Counsel knew of the prior non-identification, and the detective who administered the identification procedure brought the photo array into court for examination. (*See* notes of testimony, 9/29/97 at 47.) Significantly, defense counsel had the opportunity at the hearing to cross-examine both the detective and the victim regarding the circumstances of the photo array identification procedure and the lineup procedure.¹² For unexplained reasons, however, defense counsel did not probe either witness to establish that the lineup procedure was suggestive, or tainted, or otherwise resulted in a substantial likelihood of misidentification. (*See id.* at 41-42, 44; and 83-84.) Defense counsel also did not explore the victim's credibility given her prior failure to identify appellee from the photo array. We therefore cannot find that appellee was prejudiced by the prosecutor's failure to disclose.

¶ 33 Order reversed. Case Remanded. Jurisdiction is relinquished.

¹² Given that the victim did not identify appellee from the photo array, appellee logically does not attack the photo array as defective.