IN THE SUPREME COURT OF THE STATE OF OREGON

STATE OF OREGON, Plaintiff-Respondent, Respondent on Review, v. DENNY D. GHIM, Defendant-Appellant Petitioner on Review.	Washington County Circuit Court Case No. C111491CR CA A152065 S063021

BRIEF ON THE MERITS OF PETITIONER ON REVIEW

Review the decision of the Court of Appeals
on an appeal from a judgment of the Circuit Court
for Washington County
Honorable Gayle A. Nachtigal, Judge

Opinion Filed: December 10, 2014
Author of Opinion: Sercombe, Presiding Judge
Concurring Judges: Hadlock, Judge, and Mooney, Judge pro tempore

ERNEST G. LANNET #013248
Chief Defender
Criminal Appellate Section
MORGEN E. DANIELS #075739
Deputy Public Defender
Office of Public Defense Services
1175 Court Street NE
Salem, OR 97301
Morgen.E.Daniels@opds.state.or.us
Phone: (503) 378-3349
Attorneys for Petitioner on Review

ELLEN F. ROSENBLUM #753239
Attorney General
ANNA JOYCE #013112
Solicitor General
ROBERT M. WILSEY #085116
Assistant Attorney General
400 Justice Building
1162 Court Street NE
Salem, OR 97301
robert.wilsey@doj.state.or.us
Phone: (503) 378-4402
Attorneys for Respondent on Review

……continued

JULIE E. MARKLEY #000791
KRISTINA J. HOLM #112607
1120 NW Couch Street, 10th Floor
Portland, OR 97209-4128
Phone: (503) 727-2000
JMarkley@perkinscoie.com
KJHolm@perkinscoie.com
Attorneys for *Amicus Curiae*
American Civil Liberties
Union of Oregon, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional and Statutory Provisions

Other Authorities

PETITIONER'S BRIEF ON THE MERITS

STATEMENT OF THE CASE

Defendant's case presents an issue of first impression in Oregon: whether a prosecutor conducts a search for purposes of Article I, section 9, when he or she subpoenas years of a person's account information from that person's banks.

Questions Presented and Proposed Rules of Law

First Question Presented. Does a person have a constitutionally protected right to be free of unreasonable governmental scrutiny of years of records detailing all transactions in or out of his or her bank accounts?

First Proposed Rule of Law. A person has an Article I, section 9, privacy interest in his or her bank records because those records disclose sensitive details about a person's financial circumstances, history, and decision-making, and about a person's daily movements, personal preferences, opinions, and beliefs.

Second Question Presented. When a person employs an agent or purchases services from a business, and in the course of the agency or service relationship shares private financial information with the agent or service provider that the entity records and aggregates, does that sharing of information extinguish the person's privacy interest in the information?

Second Proposed Rule of Law. Privacy does not require secrecy. A person's protected privacy interest in his or her financial information survives the sharing of information that is a necessary part of using the services of a bank or other financial services provider.

Nature of the Proceeding

Defendant was convicted of theft for taking part in a "Ponzi"[1]-type scheme in which his wife, codefendant, represented that they were making significant profit by "flipping"[2] houses and took others' money to "invest" in the scheme. After a citizen reported that he thought something suspicious was going on, the Oregon Division of Finance and Securities obtained six years' worth of defendants' bank records through an administrative subpoena and then turned the records over to the Tigard police. Defendant's prosecution resulted from law enforcement review of the subpoenaed bank records.

Before trial, defendants argued that the bank records evidence must be suppressed because the state had violated Article I, section 9, by obtaining those records absent exigent circumstances and probable cause, or some other

---

[1] A Ponzi scheme is a "fraudulent investment operation where the operator * * * pays returns to its investors from new capital paid to the operators by new investors, rather than from profit earned by the operator." *See* https://en.wikipedia.org/wiki/Ponzi_scheme (accessed July 5, 2015).

[2] "Flipping" is a term used to describe the purchase and quick resale of a revenue-generating asset, frequently real estate. *See* https://en.wikipedia.org/wiki/Flipping (accessed July 5, 2015).

exception to the warrant requirement. The trial court denied suppression, ruling that defendants had no constitutionally protected privacy interest in the records. During trial, defendants renewed their privacy argument and also argued that the administrative subpoena had not been correctly executed. The trial court allowed a continuance, giving the state the opportunity to re-subpoena the records. The district attorney obtained the same set of records using a criminal action subpoena rather than a securities division administrative subpoena. Defendant again sought suppression which the trial court denied.

Defendant raised the Article I, section 9, challenge again on appeal. The Court of Appeals affirmed the trial court's ruling, holding that under this court's decision in *State v. Johnson*, 340 Or 319, 336, 131 P3d 173 (2006), defendant had no privacy interest in his bank records because the records were "created in the course of the bank's regular operations. And the bank records—memorializing transactions to which the bank was a party and tracking the bank's processing of money into and out of various accounts—were held and maintained by the bank for the bank's own purposes." *State v. Ghim*, 267 Or App 435, 440-43, 340 P3d 753 (2014).

Statement of Facts

Trial Facts

Defendant convinced retired mortgage broker Marvin to invest in his wife's (codefendant's) business conducting real estate short sales.

Tr 376, 380, 384-87. forwarded $16,000 to defendants with the understanding that he would get a significant return on his investment in 30-60 days. Tr 384-86.

As time passed and no money appeared, became concerned. Tr 393. Codefendant promised information regarding the short sale but never provided it. Tr 395. She led to believe that he would receive a wire transfer that never occurred. Tr 397-98. She wrote a check that bounced after claiming that the deal had fallen through. Tr 401-03. Defendants eventually returned all money owed to Tr 406.

Mrs. called the police who suggested they contact an attorney. Tr 429-32. The attorney put the in touch with Ruth Johnson, an investigator at the Oregon Division of Finance and Securities, the state agency that enforces regulations concerning the sale of securities in Oregon. Tr 431, 485. Johnson began investigating defendant and codefendant. Tr 483-84.

Johnson subpoenaed records for the years 2006 to 2009 from bank accounts associated with codefendant at Bank of America and Wells Fargo. Tr 486-89; subpoenas, TCF. When Johnson discovered from those records that the money "was not used for what the had anticipated[,]" Johnson began reviewing the materials for other victims of fraud. Tr 484.

Based on the bank records, Johnson identified other people who had invested money with codefendant. Tr 490. All of the named victims in this case were identified as a result of Johnson's administrative subpoena of codefendant's bank records. Tr 491. In 2010 or 2011, Johnson subpoenaed a second round of records to see if defendants were continuing to receive "investments." Tr 490-92.

Among the victims[3] that Johnson discovered were the and the Tr 491. Ben lost his $60,000 investment in codefendant's non-existent house-flipping scheme. Tr 99-100; 112-17. Julieta lost her $6,000 investment in the scheme. Tr 172-83.

Procedural Facts

As noted above, Johnson turned over the records she had obtained via administrative subpoenas to the police. Tr 512-13. In a motion in limine, defendants challenged the bank records' admissibility on the basis that Johnson's subpoenas violated Article I, section 9. Tr 272-85. The trial court disagreed and denied the motion to exclude the records. Tr 285.

[3] Defendant's mother, was also a named a victim. Indictment, TCF. In reviewing the subpoenaed records, Johnson discovered that money in accounts that were meant to benefit was being misused. Tr 497-98. Defendant was acquitted of all counts in which was the named victim. Judgment, TCF.

During trial, defendants moved to suppress the records under Article I, section 9, and on the basis that Johnson had not complied with the statutory requirements in issuing her administrative subpoenas. Tr 443, 518-19; Motion to Suppress, TCF. The trial court ruled that the subpoenas had indeed been improperly served and therefore the records had not been lawfully obtained. Tr 444. The court continued the trial for several weeks to give the state an opportunity to re-subpoena the records properly. Tr 444-45. The district attorney re-subpoenaed the same records under ORS 136.583, the criminal witness subpoena statute. Tr 520; Exhibits 138, 138A, 139, 139A, TCF. The trial court admitted those records when the trial resumed. Tr 520-24. The court convicted defendant of one count of first-degree theft and one count of aggravated first-degree theft. Tr 1044-45; Judgment, TCF.

Summary of Argument

A government action that infringes upon a person's privacy interest by impairing his or her right to be free from government scrutiny is a search under Article I, section 9. A person has a privacy interest in bank records even though the records are shared with and held by a third party. A warrantless search is unreasonable unless the search is supported by probable cause and an exigency or by some exception to the warrant requirement. The prosecutor's warrantless acquisition of years of defendant's bank records was an unreasonable search.

The freedom from scrutiny that is protected by Article I, section 9, turns in large part on social and legal norms. To assess whether a person has a privacy interest in information shared with a third party or held by a third party, this court should analyze the context of the disclosure of the information to the third party, and the acquisition of the information by the state in light of the social and legal norms governing the type of information at issue. Factors that aid in that analysis are (1) the nature and scope of the information; (2) the purpose and necessity of the disclosure; and (3) the degree to which access to the information is restricted. That analysis shows that bank records do fall within the protective ambit of Article I, section 9.

In *State v. Johnson,* this court held that the defendant had no cognizable privacy interest in records kept by his cellular phone provider of numbers dialed from his account because the records were the telephone company's business records and because the defendant had voluntarily disclosed the numbers dialed to the phone company by dialing them. *Johnson* does not control here. The bank records at issue in this case are distinguishable from the phone records in *Johnson*. Alternatively, *Johnson* was inadequately reasoned as to the third party records question and this court should decline to follow it here.

The state violated defendant's right to be free from unreasonable government scrutiny when it acquired years of his bank records without a warrant and without any probable cause that he was engaged in criminal

conduct. This court should recognize that defendant had a protected privacy interest in his records and reverse the decision of the Court of Appeals.

ARGUMENT

I. Introduction

Defendant's case asks this court to decide whether a person has a constitutionally protected privacy interest in bank records, even though (1) the bank is creator and a custodian of the records; and (2) the individual has shared ostensibly private information with the bank to allow the bank to create and maintain those records. This court should recognize that Article I, section 9, protects a privacy interest in such records. Privacy is not an either/or proposition that is "extinguished by the sharing of information with select others, as privacy is not an indivisible commodity [that is] limited to secrecy." *ABA Standards for Criminal Justice, Third Ed, Law Enforcement Access to Third Party Records* http://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/third_party_access.authcheckdam.pdf (accessed July 5, 2014).

At trial and in the Court of Appeals, defendant contended that the government's use of a subpoena to obtain years of his bank records absent probable cause and an exigency violated his right under Article I, section 9, of

the Oregon Constitution to be free from unreasonable government search and seizure. Article I, section 9, provides in part:

> "No law shall violate the right of the people to be secure in their persons, houses, papers, and effects against unreasonable search, or seizure * * *."

Article I, section 9, protects both privacy and possessory interests against certain intrusions by the state, *i.e.*, unreasonable searches. *State v. Owens*, 302 Or 196, 206, 729 P2d 524 (1986). "A 'search' occurs when a person's privacy interests are invaded." *Owens*, 302 Or at 206. A privacy interest is "an interest in freedom from particular forms of scrutiny." *State v. Campbell*, 306 Or 157, 170, 759 P2d 1040 (1988). The privacy interest is defined by an objective test of whether the state's conduct "would significantly impair an individual's interest in freedom from scrutiny * * *." *State v. Dixson/Digby*, 307 Or 195, 211, 766 P2d 1015 (1988). State scrutiny that does not invade a person's privacy interest is not a search under Article I, section 9. *Campbell*, 306 Or at 170.

To determine whether the state's acquisition of defendant's bank records violated defendant's Article I, section 9, rights, this court must first determine whether he had a privacy interest in his bank records such that the state's subpoenas constituted a search. If the use of the subpoenas to gain defendant's bank records was a constitutionally significant search, then this court must decide whether it was reasonable.

II. Under Article I, section 9, government scrutiny constitutes a constitutionally significant search when that scrutiny, viewed in context, breaches social and legal norms.

A. A search is a government action that infringes on an individual's privacy interest, which is an interest in freedom from particular forms of scrutiny.

Under Article I, section 9, a government action is a search when the action, "if engaged in wholly at the discretion of the government, will significantly impair 'the people's' freedom from scrutiny." *Campbell*, 306 Or at 171. This test is objective. *State v. Wacker*, 317 Or 419, 425, 856 P2d 1029 (1993). It is based on the "general privacy interests of 'the people' rather than the privacy interests of particular individuals." *State v. Tanner*, 304 Or 312, 320, 745 P2d 757 (1987). "[T]he privacy protected by Article I, section 9, is not the privacy that one reasonably expects but the privacy to which one has a *right*." *Campbell*, 306 Or at 165 (emphasis in the original).[4] In the context of a

[4] This court developed that objective test for evaluating the government's conduct with respect to people's privacy to distinguish Article I, section 9's protection from the *subjective* Fourth Amendment test drawn from Justice Harlan's concurrence in *Katz v. United States*, 389 US 347, 361, 88 S Ct 507, 19 L Ed 2d 576 (1967) (Harlan, J., concurring): *viz.*, a person has a privacy interest if "[the] person [has] exhibited an actual (subjective) expectation of privacy and, second, * * * the expectation [is] one that society is prepared to recognize as 'reasonable.'"). In *Campbell*, this court "expressly rejected" that "reasonable expectation of privacy" formulation because it "expressed a conclusion rather than a starting point for analysis[,]" and because it depends on subjective, shifting notions of privacy. *Campbell*, 306 Or at 164-65. Justice Harlan himself later noted the shortcomings of the "reasonable expectation of privacy" test in *United States v. White*, 401 US 745, 786, 91 S Ct 1122, 28 L Ed 2d 453 (1971) (Harlan, J., dissenting) (footnote omitted):

warrantless search, the state bears the burden of proving that the search did not violate a protected interest. *State v. Unger*, 356 Or 59, 75, 333 P3d 1009 (2014).

"[T]he freedom from scrutiny that Article I, section 9, protects turns in large part on 'social and legal norms of behavior.'" *State v. Howard/Dawson*, 342 Or 635, 642, 157 P3d 1189 (2007) (quoting *Campbell*, 306 Or at 170). Such norms do not govern the scope of the constitutional provision—to the contrary, the constitution plays a substantial role in shaping those norms—but social and legal norms of behavior serve "to clarify the nature of the interest protected by Article I, section 9." *Campbell*, 306 Or at 171. The ultimate question "'is whether, if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society.'" *Campbell*, 306 Or at 171 n 8 (quoting Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn L Rev 349, 403 (1974)).

> "While [the 'expectation of privacy'] formulations represent an advance over the unsophisticated trespass analysis of the common law, they too have their limitations and can, ultimately, lead to the substitution of words for analysis. The analysis must, in my view, transcend the search for subjective expectations or legal attribution of assumptions of risk. Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present."

This court assesses whether a person has a protected privacy interest "in light of the particular context in which the government conduct occurred." *State v. Meredith*, 337 Or 299, 306, 96 P3d 342 (2004). When the privacy interest at issue is an interest in something that has been turned over to a third party, the "legal relationship" between the person asserting the interest and the entity to which the item is given informs the question of whether the person retains a constitutionally protected privacy interest in the item. *Howard/Dawson*, 342 Or at 642-43. *See also Tanner*, 304 Or at 317 (asking "whether the entrustment of an effect to another person is sufficient to establish an Article I, section 9, right against an unlawful search that uncovers the effect."). When the asserted privacy interest is in information, the nature and scope of the information are integral to the assessment of whether a privacy interest exists.

B. To assess whether a person has a protected privacy interest in information shared with or held by a third party, this court should examine the nature and scope of the information at issue, the context in which the information is shared, and the nature of the relationship between the person asserting the interest and the third party.

This court has not squarely decided whether a person retains a constitutionally protected privacy interest in information that is divulged to a third party or whether a person has a privacy interest in the records that a third

party keeps about the person and his or her information in the course of a business relationship.

This court should rely on principles it identified in *Howard/Dawson* and *Meredith* to evaluate the question. Examination of the nature of the relationship between the individual and the third party and the context in which the information was shared, the records were created, and the records were accessed by the state, will illuminate the nature of the privacy interest that exists. In addition, as part of that contextual inquiry, the nature and scope of the information at issue are critical.

1. The court's focus in *Johnson* on possession and control appears to deviate from the contextual analysis that governs *Howard/Dawson* and *Meredith*.

This court's existing case law concerning the privacy of third party records is scant. The only decision that deals directly with the issue is *State v. Johnson*, 340 Or 319, in which this court analyzed and rejected in one brisk paragraph the defendant's claim that the state's warrantless acquisition of his cellular telephone call records violated Article I, section 9. *Id.* at 336. The principal reason that the *Johnson* court gave for its decision was that the records at issue were "generated and maintained" by the cellular telephone provider for its own business purposes, and that the defendant therefore had no cognizable privacy interest in the records. *Id.* The rationale of that decision seems to be that

defendant had no *possessory* interest in the records and therefore no cognizable Article I, section 9, interest in them.

The *Johnson* holding comports with the United States Supreme Court's Fourth Amendment[5] approach to phone records and bank records. The starting and ending point for that approach focuses on the fact that the person claiming a privacy interest in the information does not have exclusive possession of the information. Put simply, the federal third party rule states that a person has no cognizable privacy interest either in information "voluntarily" shared with other people or entities, or in a third party's business records relating to that information. *United States v. Miller*, 425 US 435, 440-43, 96 S Ct 1619, 48 L Ed 2d 71 (1976) (holding that the defendant had no Fourth Amendment privacy interest in bank records because such records were not "private papers" owned by the defendant, and because the information contained in them was exposed to others in the course of bank business); *see also Smith v. Maryland*, 442 US 735, 741-46, 99 S Ct 2577, 61 L Ed 2d 220 (1979) (relying on *Miller* to hold that there is no Fourth Amendment "legitimate expectation of privacy" in

---

[5] The Fourth Amendment to the United States Constitution provides:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

records of calls dialed from a telephone because the numbers are voluntarily conveyed to the telephone company and the company keeps the records for its own business purposes).

The "voluntarily-shared" approach conflates privacy with secrecy and is unhelpfully black and white, especially given the gradations of digital grey that have evolved since the Supreme Court decided *Miller* and *Smith*. Professor LaFave roundly criticizes the federal third party rule for ignoring the possibility that a person is entitled to freedom from government scrutiny in information held by others:

> "The result reached in [*Miller*] is dead wrong, and the [Supreme Court's] woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection the Court had developed in *Katz*. A bank depositor's informational control over his financial transactions deserves Fourth Amendment protection surely as much as occupancy of telephone booths. Especially in light of the massive recordkeeping of personal financial transactions, unrestricted government access to bank records poses a severe threat to civil liberties and privacy, and this is true in spades as to the post-9/11 high-volume government acquisition of financial records. * * *.
>
> "The Court's assertion in *Miller* that there can be no protected Fourth Amendment interest where there is neither ownership nor possession is contrary to the purposes underlying the Fourth Amendment, the teachings of *Katz*, and the realities of modern-day life. Ownership and possession are property concepts which, the Court wisely concluded in *Katz*, cannot serve as a talismanic solution to every Fourth Amendment problem, and which surely do not lead to the proper solution in this context. Unquestionably, the Fourth Amendment's drafters were * * * concerned with privacy in the sense of control over information."

Wayne R. LaFave, 1 *Search and Seizure* § 2.7(c), 970-71 (5th ed 2012) (internal citations and quotation marks omitted).[6]

For the reasons Professor LaFave notes and the reasons explained below, this court should not follow the Fourth Amendment approach in gauging Article I, section 9, protection of bank records. Unlike the Fourth Amendment's focus on the *un*reasonableness of a person's expectation that a third party will not share information that the person has not jealously maintained exclusive possession or ownership over, Article I, section 9, has a different focus. The predicate concern is not whether a person can thwart all dissemination of private information, but whether the people have the right to prevent unreasonable government scrutiny of that information.

Given the arguably broader protection afforded under the state constitution, the all-or-nothing, binary formulation of the federal third party doctrine is of limited utility in assessing whether and to what degree Article I, section 9, protects bank records. This court has never adhered to the proposition that a person extinguishes his or her privacy interest in a thing or space by sharing it with others. Article I, section 9 does not demand that the people must hide or conceal their affairs before claiming that they are "private." To the

---

[6] In the cited section, Professor LaFave thoroughly explores what he calls the "pernicious" and "lamentable" third party doctrine, identifying many of the problems and pitfalls that the doctrine created and amplifies. LaFave, 1 *Search and Seizure*, § 2.7(c), 966-983.

contrary, levels of privacy vary based on the relationships among people, places, and entities, and their conduct with respect to the shared matter. *See, e.g.*, *Tanner*, 304 Or at 321-22 (discussing different levels of privacy interests held by guests in a house as opposed to residents of the house); *Campbell*, 306 Or at 166-67 (discussing the degree to which a person acting in the public view has a privacy interest in his or her conduct with respect to police observation of that conduct); *Howard/Dawson*, 342 Or at 642-43 (a person who wholly gives up to another the right to control the item in which the privacy interest is asserted gives up his or her privacy interest in the item as though the item had been abandoned); *Meredith*, 337 Or at 306-07 (government employee did not have a privacy interest in her work-related activities and location on work time while she was using employer-owned property).

2. In *Meredith* and *Howard/Dawson*, this court used contextual analysis in light of social and legal norms to evaluate the degree of protection that Article I, section 9, provided.

The approach in *Meredith* and *Howard/Dawson* provides analysis that this court should amplify and apply to bank records. To determine whether a person has a privacy interest in information shared with a third party, this court should consider the nature of the information, the context of the disclosure of the information—including the relationship between the person claiming the privacy interest and the third party that receives the information, and the context

of the conduct by which the state accessed the information. *Meredith*, 337 at 306; *Howard/Dawson*, 342 Or at 642-43.

The issue in *Meredith* was whether the defendant, a United States Forest Service (USFS) employee, had a privacy interest in her movements and location while she was using a work truck during the work day. 337 Or at 301-02. As part of a criminal arson investigation, USFS law enforcement agents attached a transmitter to the USFS truck that the defendant usually used and were able to follow her and observe what she did over the course of the work day. *Id.* at 302. They saw her start fires, and the state charged her with arson. *Id.* The trial court ruled that under *Campbell*, 306 Or 157, the USFS use of the transmitter was a search, but that it was reasonable because the defendant's employer had permitted it. *Meredith*, 337 Or at 303. In this court, the *Meredith* defendant argued that under *Campbell*, *any* secret government use of a transmitter to track a person's movements "significantly impaired the interest of 'the people' to be free from scrutiny" and was therefore a constitutionally offensive search. *Meredith*, 337 Or at 305.

This court rejected that contention, explaining that whether a defendant had a protected privacy interest in any given situation must be assessed case by case "in light of the particular context in which the government conduct occurred." *Id.* at 306. This court distinguished *Meredith* from *Campbell* in light of the *context* of the government action. *Id.* In *Campbell*, the court pointed out,

the transmitter had been placed by trespassing on the defendant's personal vehicle and the officers had subjected the defendant to "pervasive and constant examination of his movements and location throughout his daily life[,]" thereby observing much that would normally have been inaccessible to the public or to government officials. *Id.* In *Meredith*, by contrast, the defendant was observed in the employment context with her employer's permission (indeed, by other employees of her employer)—she "did not have a protected privacy interest in keeping her location and work-related activities concealed from the type of observation by her employer that the transmitter revealed." *Id.* at 307. The court held that neither the attachment of the transmitter nor the subsequent monitoring of the defendant invaded a privacy interest. *Id.* The outcome in *Meredith* turned on the context of the government action at issue—a state employer observing an employees' ostensibly private but actually unprotected information, *i.e.*, her movements and activities over the course of her work day.

This court employed similar reasoning in *Howard/Dawson*, 342 Or 635. There, the defendants claimed a privacy interest in garbage that they had put out for collection by the garbage company and which the company had then turned over to the police. *Howard/Dawson*, 342 Or at 638. The defendants recognized that they had "lost control of the garbage once the sanitation company had picked it up[,]" but maintained that their privacy interest in the garbage survived the loss of their possessory interest. *Id.* at 640. The defendants rested

their argument on *Campbell*, arguing that the determining factor was that the officers' acts "if engaged in wholly at the discretion of the government, [would] significantly impair the people's freedom from scrutiny." *Id.* at 642 (internal quotation marks and citations omitted).

As it did in *Meredith*, this court relied on a contextual approach to resolve the question of whether the defendants retained a constitutionally protected privacy interest in the information (*i.e.*, the discarded garbage) at issue: the court determined once again that the *relationship* between the defendants and the entity to which the information was surrendered "control[led] the question[.]" *Howard/Dawson*, 342 Or at 642. The court explained further that the "context in which the challenged action occurs" is key to the inquiry. *Id.* Because the defendants had agreed with the garbage company that they would essentially abandon their property on the curb and that the garbage company would pick it up and dispose of it, the court determined that the defendants had abandoned both their possessory and privacy interest in the materials in question. *Id.* at 642-43. The nature of the agreed-upon relationship, *i.e.*, the purpose of the disclosure of the information, between the defendants and the sanitation company was the key to the court's decision.

3. This court should rely on the contextual analysis it used in *Meredith*, *Howard/Dawson*, and *Campbell* to determine that Article I, section 9, protects a person's privacy interest in bank records.

Pulling together analysis from *Campbell*, *Meredith*, and *Howard/Dawson* yields a practicable analytical framework for evaluating whether a person retains a privacy interest in information disclosed to others and resulting third-party records. The larger question, from *Campbell*, is "whether the practice, if engaged in wholly at the discretion of the government, will significantly impair 'the people's' freedom from scrutiny." *Campbell*, 306 Or at 171. But the analysis of that question does not end with a yes or no answer. Rather, it rests on evaluation of social and legal norms and requires that courts examine the "applicable legal and factual context" in each case to determine whether the government conduct at issue actually does impair the people's freedom from scrutiny. *Howard/Dawson*, 342 Or at 642.

Consideration of contextual factors is necessary in the application of the relationship-based analysis from *Meredith* and *Howard/Dawson*. Contextual

factors[7] that could prove helpful include (1) the nature and scope of the information in question; (2) the purpose of the disclosure and the degree to which it is reasonably necessary to participate in the ordinary activities of daily life; and (3) whether and how the information is accessible to others aside from the third party and the state, including the degree to which existing law protects or restricts access to the information. In essence, these factors are more specific ways to examine the "social and legal norms" that are the everyday manifestations of the privacy that Article I, section 9, protects.

III. Warrantless scrutiny of years' worth of an individual's bank records in a criminal prosecution constitutes a search under Article I, section 9.

A. Social and legal norms demonstrate that Article I, section 9, protects and individual's privacy in financial information against government scrutiny.

Social and legal norms of behavior help courts to discern the outlines of the privacy interests that Article I, section 9, protects. *Campbell*, 306 Or at 170; *Howard*, 342 Or at 642. The manners, mores, and laws that guide and regulate

---

[7] These factors are borrowed, with alteration, from Stephen Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 Iowa L Rev Bull 39, 50-51 (2010-2011). Henderson developed his framework in the context of crafting American Bar Association (ABA) practice standards regarding law enforcement access to third party records in the Fourth Amendment context, but the factors should be useful in the Article I, section 9, context as well. *Id.* at 50. *See also ABA Standards for Criminal Justice*, Third Ed, *Law Enforcement Access to Third Party Records*. http://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/third_party_access.authcheckdam.pdf (accessed July 5, 2014).

conduct among individuals inform what types of governmental investigative conduct are constitutionally acceptable. *See Campbell*, 306 Or at 170 ("One explanation for the absence of a constitutionally protected interest against certain forms of government scrutiny may be the absence of any freedom from those forms of scrutiny in society at large. The reason that the observations of a police officer who is standing in a public place infringe no privacy interest may be that there is no generally recognized freedom from such scrutiny by private individuals. Such observations by the police would thus not significantly reduce the freedom from scrutiny available to 'the people.'").

The inquiry is whether the government conduct at issue would offend social or legal norms if private citizens engaged in the same conduct. If, for example, a police officer overhears a sidewalk conversation and makes investigational hay out of what she hears, her conduct offends neither privacy nor the constitution. No social norm dictates that we stop up our ears so as not to overhear public conversations, and the police may act on information that is publicly available. But where the officer takes extra steps to overhear that conversation, such as standing underneath a bedroom window, she violates the social norm against eavesdropping in addition to violating protected privacy interests.

Here, where bank records are concerned, numerous social norms are relevant. Those norms generally inhibit people from prying into the financial

information of others. It may be that bank employees can access a person's financial records,[8] but the general public cannot. It is considered rude to ask people about their money.[9] The conventions against prying into financial matters are like the conventions against eavesdropping—expressed in manners and customs and grounded in a longstanding societal concern for individual privacy. Clearly, an individual would violate these norms by obtaining and scrutinizing years of a person's bank records. Such norms suggest that for the government to do so violates the privacy guaranteed by Article I, section 9.

---

[8] Arguably, social norms bar even bank employees from certain types of access of customer records. It is unquestionably within the employee's duties to process daily transactions, but most bank customers would be discomfited upon learning, for example, that a bank employee had assembled a detailed report analyzing the customer's spending habits over the life of his or her relationship with the bank, or if a bank employee contacted them and offered advice or comment about loans or purchases. Such conduct would fall well outside the social conventions regarding a bank's interaction with individuals.

[9] *See, e.g.*, Diane Harris, *Kids, Money, and Good Manners*, Parenting Magazine, http://www.parenting.com/article/kids-money-and-good-manners (accessed July 6, 2015) ("Young children understand the concept of privacy as it relates to their bodies, so you can use this notion to explain our society's taboos about talking about money."); David Lazarus, *Mind Your Money Manners: Financial Etiquette Rules*, Interview with Liz Weston, Marketplace Business, http://www.marketplace.org/topics/business/mind-your-money-manners-financial-etiquette-rules (accessed July 6, 2015) (discussing changing "rules": "Something that hasn't changed: asking someone how much they make or how much they've paid for something. 'This is something that's absolutely personal and absolutely private and it's not appropriate to ask [about it.]'").

The conduct of financial institutions also illustrates the norms of financial privacy. Banks and credit unions pledge to protect information, to keep it safe and use it only as directed.[10]

Legal norms also show that Article I, section 9, protects bank records that are maintained and held by the bank. First, Oregon has a statute directly on point: ORS 192.583 to 192.607, "Private Financial Records." That statute delineates the limited ways that the government can access people's financial records. It provides several civil causes of action against those who violate the statute, ORS 192.606, and it contains an exclusionary remedy. ORS 192.606(b). Materials obtained in violation of the statute are inadmissible in "any" court proceeding. *Id.* This statute does not *create* a privacy interest in financial records. Rather, like the social norms discussed above, it mirrors the existence of the right and reveals some of its contours.

In this respect, the private financial records statute is like those statutes that set forth how the state must go about obtaining search warrants and wiretaps. ORS 133.545 (setting forth the requirements for obtaining search warrants); ORS 133.724 (setting forth the requirements for state interception of

---

[10] The record in this case does not reveal the precise nature of defendant's dealings with Bank of America and Wells Fargo, the banks involved here, but it is reasonable to suppose that he enjoyed the same level of commitment to security and privacy that banks promise in their promotional literature and on their websites. *See, e.g.*, https://www.wellsfargo.com/privacy-security/ (accessed July 10, 2015).

communications). Those statutes do not *create* the search warrant requirement or the requirement that law enforcement fulfill certain conditions before obtaining a wiretap. Article I, section 9, does that. Those statutes recognize the right to privacy and instruct the state how to give the right effect.

Legal norms in sister states suggest that the right to privacy includes the right to privacy in bank records. Other jurisdictions have interpreted their constitutional search and seizure provisions to protect bank records against state scrutiny. *See, e.g.*, *Burrows v. Superior Court*, 13 Cal 3d 238, 529 P2d 590 (1974); *People v. Lamb*, 732 P2d 1216, 1220-21 (Colo 1987); *Winfield v. Div of Pari-Mutuel Wagering*, 477 So 2d 544, 548, 10 Fla L Weekly 548 (1985); *People v. Jackson*, 116 Ill App 3d 430, 435, 452 NE 2d 85 (1983); *State v. McAllister*, 184 NJ 17, 29-33, 875 A2d 866 (2005); *State v. Thompson*, 810 P2d 415, 416-18 (Utah 1991); *State v. Miles*, 160 Wash 2d 236, 243-44, 156 P3d 864 (2007). [11] Federal legislators, too, have given shape to these legal norms. In the wake of *Miller*, the United States Congress enacted the Right to Financial Privacy Act, 12 USC §§ 3401-422, to codify the privacy interest in bank records. *See* Nancy Kirschner, *The Right to Financial Privacy Act of 1978—The*

[11] For a detailed account of how the fifty states treat third party records, under both the federal and individual state constitutions, see Stephen Henderson, *Learning From All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath U L Rev 373 (2005-2006).

Congressional Response to United States v. Miller*: A Procedural Right to Challenge Government Access to Financial Records*, 13 U Mich J L Reform 10 (1979-1980) (describing the history of the Fourth Amendment third party doctrine and the Right to Financial Privacy Act).[12]

Social and legal norms regard financial information as private. These norms spring from a longstanding cultural and legal tradition of informational privacy and control that has existed at least since the framing of the Fourth Amendment. *See, e.g.*, Note, *Government Access to Bank Records*, 83 Yale L J 1439, 1439, 1456-59 (1974) (discussing framers' efforts to incorporate case law that dealt with protection of informational privacy into the Constitution.).

B. The sharing of financial information with a financial services provider does not "waive" the individual's right to privacy in that information.

No Oregon court has held that a person who shares personal information with another categorically gives up all privacy interest in that information merely by sharing it. The government cannot force disclosure of something private merely by demonstrating that the person who controls it has shared it with someone else. Rather, Oregon law recognizes that gradations of privacy

---

[12] Oregon's own SB 708 (1977), "An Act Relating to Privacy of Financial Records," was enacted in July of 1977, little more than a year after the Supreme Court decided Miller. At that time, this court had not yet explicitly dissociated Article I, section 9, privacy analysis from Fourth Amendment analysis. It is possible that the Oregon legislature sought through the financial privacy act to protect Oregonians in the event that this court chose to follow the United States Supreme Court's approach in *Miller*.

exist, and that a person's privacy interest can persist absent exclusive control or possession, depending on context. *See, e.g.*, *Tanner*, 304 Or 312, 745 P2d 757 (1987) (entrustment of an effect to another does not extinguish a person's privacy interest in that effect); *State v. Cook*, 332 Or 601, 608-09, 34 P3d 156 (2001) (the defendant's Article I, section 9, privacy interest in effects was not extinguished by his disclaimer of ownership).

An individual's control over personal information is analogous to his or her control over personal effects. In an increasingly digital world, very little information is exchanged in traditional, tangible forms. Constitutional protection should shelter personal information stored and manipulated by third parties to the same degree that it protects personal information stored in more traditional formats that existed in the 18th and 19th centuries. Just as Article I, section 9, would protect a handwritten, annotated register in a checkbook, it should protect the significantly more detailed digital registry that banks now automatically compile.

C. The prosecutor's warrantless acquisition of defendant's bank records was an unreasonable search.

1. The prosecutor's acquisition of defendant's bank records was a search because it infringed on defendant's privacy interest in those records by impairing his right to be free from state scrutiny.

Based upon consideration of the social and legal norms discussed above and upon examination of the specific context within which the government

accessed defendant's bank records, it is apparent that the government's action was a "significant limitation on freedom from scrutiny." *Campbell*, 306 Or at 172. The government's action laid bare a précis of several years in the life of defendant and his family in multifarious detail. Short of wiretaps or full person-to-person surveillance, few tools exist to conduct a more comprehensive surveillance than that enabled by a full set of the kind of detailed bank records that the prosecutor obtained.

Defendant engaged in a banking relationship with Bank of America and Wells Fargo. He entrusted his money and his personal information to those entities in exchange for their assistance keeping track of his money.[13] He did not abandon property to them, nor did he provide money and information to them with the intent, expectation, or understanding that they would make his entrustments public. The government obtained a significant swath of defendant's bank records first through an improperly executed subpoena that was based on a single citizen report of possible wrongdoing (the securities division subpoenas), and then through a second unlawful subpoena process (the prosecutor's criminal subpoenas) that was based on the fruits of the first flawed subpoena process (the securities division subpoenas). Given that context, and applying the factors suggested in section II(B) in defendant's case makes clear

---

[13] The record does not contain the details of any contractual arrangements defendant and codefendant may have made with their banks.

that Article I, section 9, protects privacy in bank records and that the government's search was unreasonable.

Defendant suggested, *supra*, three factors to aid this court in assessing whether a person has a privacy interest and whether government invasion of that interest is unreasonable: (1) the nature and scope of the information in question; (2) the purpose of the disclosure and the degree to which it is reasonably necessary to participate in the ordinary activities of daily life; and (3) whether and how the information is accessible to others aside from the third party and the state, including the degree to which existing law protects or restricts access to the information.

Applying those factors in the context of bank records shows that a person does indeed have a protected privacy interest in such information. First, the nature and scope of the information contained in bank records is personal, detailed, and broad. Bank records now contain far more information both in quantity and in kind than they did in the past. Not only can the entity that surveys a person's bank records learn all about his or her finances, the entity can glean countless details about other aspects of that person's private life as well.

Second, a person who wishes to participate in everyday life has little choice whether to share financial information with a bank or financial institution, and in fact, *must* do so to engage in many ordinary activities such as

securing a mortgage to buy a house, receiving a paycheck from an employer who requires direct deposit, getting a loan for a car or to start a business, renting an apartment or business premises, etc. The reason a person discloses that information is not to ensure that the bank can keep tabs on the person's activities, but so that he or she can take part fully in the ordinary activities of daily life.

Third, the information contained in bank records is typically not readily accessible to others outside the bank or the government. Unlike, say, a conversation held on a city sidewalk or activities conducted in plain view in a parking lot, the information in bank records is generally not open to members of the public. To the extent that it is shared outside the bank, it is piecemeal: a person may, for example, write a check to the city of Salem to pay parking tickets, thereby sharing the content of the check with the city's employees who process the payment, but the data contained in the check (number of parking tickets, that the person incurred parking tickets) is not broadcast to the world. And it is indisputable that existing laws of several kinds protect bank records, both in Oregon and in the nation at large.

Taken together, these factors support the determination that bank records fall within Article I, section 9's protection of the people from unreasonable government scrutiny. The ease and depth of the access to such records that is

now readily available to the government renders that access invasive. The acquisition of the bank records in this case was a search.

2. The prosecutor's acquisition of six years of defendant's bank records was an unreasonable search.

Because the prosecutor's use of a criminal subpoena to obtain defendant's bank records was a search, it was subject to the reasonableness requirement of Article I, section 9. A search is reasonable if it is supported by a warrant, justified by an exception to the warrant requirement, or conducted pursuant to a properly authorized administrative scheme. *See Nelson v. Lane County*, 304 Or 97, 103-05, 743 P2d 692 (1987) (discussing the purpose and parameters of properly authorized administrative searches). If the search is not supported by a warrant, the state bears the burden of proving that it was reasonable. *State v. Tucker*, 330 Or 85, 87, 997 P2d 182 (2000); ORS 133.693(4) (where the evidence challenged is "seized as a result of a warrantless search, the burden of proving by a preponderance of the evidence the validity of the search is on the prosecution.").

Here, the state asserted in the trial court that defendant had no privacy interest in the records at issue and therefore that the state's conduct in obtaining the records was not a search. The prosecutor made no alternative argument concerning the reasonableness of the search, if there was a search. On appeal,

the state hewed to that same position and made no argument concerning reasonableness.[14]

Assuming that the acquisition of the bank records at issue was a search, it was unreasonable because the state had no warrant and no warrant exception applied. The prosecutor obtained the records midtrial pursuant to ORS 136.583, the criminal action subpoena statute that authorizes litigants to subpoena witnesses and documents to criminal proceedings. No exigency required the immediate acquisition of the records lest they be destroyed, and any probable cause that existed was the product of the securities division investigator's original improper subpoena of the bank records and was therefore fruit of the poisonous tree. *See State v. Delong*, 357 Or 365, 370-71, ___ P3d ___ (2015) (discussing application of the "fruit of the poisonous tree" doctrine in Oregon case law).

Nor did the state obtain the records pursuant to a properly authorized administrative search scheme. Finally, the search was unreasonable because by the state did not comply with the statute that sets forth the subpoena process

[14] The state also argued for the first time on appeal that the records at issue belonged to codefendant rather than to defendant and that defendant therefore could not properly assert a privacy interest in the records. Defendant filed a reply brief addressing that issue and the Court of Appeals rejected the state's argument. *Ghim*, 267 Or App at 439-40.

required to access bank records. It relied instead on the criminal subpoena statute.

ORS 192.586 prohibits the disclosure of financial records except under statutorily defined circumstances:

> "(1) Except as provided in ORS 192.588 [disclosure to DHS], 192.591 [disclosure to state court for court-appointed counsel evaluation], 192.593 [authorization by bank customer], 192.596 [disclosure under summons or subpoena], 192.597 [disclosure pursuant to abuse investigation], 192.598 [disclosure under search warrant], and 192.603 [procedure for disclosure to law enforcement agency] or as required by ORS 25.643 [disclosure of information on obligors by financial institutions] and 25.646 [disclosure of financial records of customers by financial institutions in support enforcement context] and the Uniform Disposition of Unclaimed Property Act, ORS 98.302 to 98.436 and 98.992:
>
> "(a) A financial institution may not provide financial records of a customer to a state or local agency.
>
> "(b) A state or local agency may not request or receive from a financial institution financial records of customers."

ORS 192.603 governs the procedure for disclosure of financial records to law enforcement, including to a district attorney's office:[15]

> "When a police or sheriff's department or district attorney's office in this state requests account information from a financial institution to assist in a criminal investigation, the financial

---

[15] ORS 192.598 provides that a financial institution "may disclose financial records of a customer to a state or local agency * * * pursuant to a lawful search warrant * * *."

ORS 192.606 provides that evidence "obtained in violation of the [private financial records statute] is inadmissible in any proceeding."

> institution shall supply a statement setting forth the requested account information with respect to a customer account specified by the police or sheriff's department or district attorney's office, for a period of up to three months prior to and three months following the date of occurrence of the account transaction giving rise to the criminal investigation. The disclosure statement required under this subsection may include only account information as defined in subsection (2) of this section. The police or sheriff's department or district attorney's office requesting the information shall, within 24 hours of making the request, confirm the request in a written or electronic message delivered or mailed to the financial institution, setting forth the nature of the account information sought, the time period for which account information is sought, and that the information has been requested pursuant to a criminal investigation.
>
> "(2) As used in this section, account information means, whether or not the financial institution has an account under a particular customers name, the number of customer account items dishonored or which created overdrafts, dollar volume of dishonored items and items which when paid created overdrafts, a statement explaining any credit arrangement between the financial institution and the customer to pay overdrafts, dates and amounts of deposits and debits to a customer's account, copies of deposit slips and deposited items, the account balance on such dates, a copy of the customers signature card and the dates the account opened or closed."

Here, the securities division investigator first accessed defendant's bank records via administrative subpoena under ORS 192.596 and ORS 59.315[16] (the

---

[16] ORS 59.315 provides in relevant part:

> "For the purpose of an investigation or proceeding under the Oregon Securities Law, the Director of the Department of Consumer and Business Services may administer oaths and affirmations, subpoena witnesses, compel their attendance, take evidence and require the production of books, papers, correspondence, memoranda, agreements or other documents or

statute that authorizes that agency to subpoena records in proceedings before the director of the Department of Consumer and Business Services). Defense Exhibit 105, TCF. However, the investigator did not serve the original subpoenas properly. The trial court excluded the records obtained through those subpoenas and continued the trial to give the state time to re-subpoena the records properly. Tr 445-46. The second time, the prosecutor subpoenaed the same records that the securities investigator had obtained, but this time under ORS 136.583, the criminal action subpoena statute. State's Exhibits 138 and 139, TCF.

The trial court should not have admitted the records. Notwithstanding that the second round of subpoenas was properly served, the subpoena process was again defective. The prosecutor did not obtain those records through the process mandated for law enforcement agencies in ORS 192.603. ORS 192.586 prohibits the disclosure of financial records except as provided in the listed exceptions. It is of no moment that ORS 192.586 contains an exception allowing disclosure under summons or subpoena. Oregon courts interpret statutes to give effect insofar as possible to every provision enacted by the legislature and to avoid unreasonable results. *See* ORS 174.010; *Carlson v. Myers*, 327 Or 213, 233, 959 P2d 31 (1998) (Durham, J., concurring)

> records which the director deems relevant or material to the inquiry."

(discussing rules of statutory interpretation in common use). If the summons/subpoena exception in ORS 192.586 is read to allow law enforcement entities to obtain private financial records without going through the procedures set forth in ORS 192.598 or 603, then both of those sections are robbed of meaning and effect. Such a result would be unreasonable and would defeat the intent of the legislature that law enforcement access to bank records be more strictly controlled than administrative or regulatory access by other agencies.

What is more, if the prosecutor had abided by the dictates of ORS 192. 603, the state would have been unable to access such a large amount of defendant's private information. The limits in ORS 192.603 indicate what the legislature considered reasonable when law enforcement officials inquire into financial information. The prosecutor's subpoena went far outside that limit and was therefore unreasonable.

In sum, the search was not reasonable under Article I, section 9. The evidence resulting from state acquisition of defendant's records should have been suppressed.

IV. *State v. Johnson* does not dictate a different result.

A. Bank records are distinguishable from the kind of cellular phone records at issue in *Johnson*.

To return to *Johnson*: in that case, the defendant moved to suppress records that the state had obtained from a number of third parties, including records of lists of calls made on his cellular telephone account. 340 Or at 335.

This court determined that the defendant had no privacy interest in the cellular telephone records:

> "Defendant clearly had a cognizable privacy interest in the content of his telephone calls. *See* ORS 133.724 (setting out requirement that police obtain judicially issued warrant to intercept a telephonic communication). However, we cannot identify a source of law that establishes that defendant also had some interest in keeping private any records kept by a third party, his cellular telephone provider, respecting his cellular telephone usage. The cellular telephone provider generated and maintained those records from the provider's own equipment and for the provider's own, separate, and legitimate business purposes (such as billing). * * *. Neither are we aware of any principle that would prevent the cellular telephone provider from responding to a proper subpoena. Defendant's assignment of error is not well taken."

Id. at 336 (internal citation omitted). That decision turned on the facts that the court could not identify a source of law to show a person has an interest in keeping third party phone records private and that the cell phone provider maintained the records for its own business purposes.

The bank records at issue here are different. First, bank records are more like the *content* of telephone calls than they are like a list of numbers dialed. A bank statement is no longer a generally anonymous list of dollar amounts in and dollar amounts out. Because of technological and organizational developments in tracking, storing, and expressing information, a bank statement can now read like a surveillance report as easily as it can a bare list of transactions. Each entry contains far more information than the simple dollar figure of the analog bank statements of forty years ago. And as with the content of telephone calls,

as this court observed in *Johnson*, there is a statute that limits the ways that the state may obtain a person's bank records: ORS 192.583 to ORS 192.607. *Johnson*, 340 Or at 336 (noting that the existence of ORS 133.724, the statute that sets out the requirements for a police wiretap, shows that there is an Article I, section 9, privacy interest in the content of telephone calls).

Third, a primary reason that banks exist is so that individuals may entrust their money to them so as to secure, organize, and monitor their financial affairs comprehensively.[17] While a bank may well have its own purposes for maintaining the kind of statements and cancelled checks at issue here,[18] those statements are generated primarily for customers' use and convenience.

Finally, as discussed *supra*, the subpoena power as exercised by the state in this case was not proper. The *Johnson* court remarked that it could see no reason why the telephone company could not comply with a "proper subpoena." Here, there was no proper subpoena. Even after the trial court gave the state a

---

[17] *See, e.g.*, https://www.bankofamerica.com/onlinebanking/online-banking.go, Bank of America's Online Banking webpage detailing the many ways its customers can access and use their account information via the internet; https://www.wellsfargo.com/online-banking/, Wells Fargo's comparable site. Bank of America and Wells Fargo are the banks from which the state subpoenaed defendant's records.

[18] And indeed is required by law to maintain certain other kinds of records: ORS Chapter 706, for instance, sets forth requirements that banks must follow with respect to recordkeeping and reporting to regulatory agencies. *See also* 12 USC § 1829b, the Bank Secrecy Act (detailing recordkeeping and recording requirements).

second chance to subpoena the records properly, the state failed to comply with the terms of ORS 192.603.

B. Alternatively, this court should decline to follow *Johnson* because it contains inadequate analysis as to the third party records issue.

In *Dixson/Digby*, 307 Or at 203, this court noted that it "is not required blindly to follow earlier 'rules' of constitutional law[,]" particularly when those rules are not supported by sufficient analysis or are justified only by dictum in earlier opinions. *See also State v. Mills*, 354 Or 350, 353-54, 312 P3d 515 (2013) (explaining that the goal of constitutional interpretation is not to "fossilize" or "freeze" constitutional rules, but to "determine the meaning of the constitutional wording, informed by general principles that the framers would have understood were being advanced by the adoption of the constitution").

The telephone records holding in *Johnson* is sparse and conclusory. It seems to be a direct analytical descendant of the Fourth Amendment third party rule as set forth in *Miller* and *Smith* (*i.e.*, an individual has no privacy interest in information "voluntarily" provided to a third party, or in records owned by a third party). But Article I, section 9, operates independently of the Fourth Amendment. *State v. Caraher*, 293 Or 741, 750-51, 653 P2d 942 (1982) (discussing independent state constitutional search and seizure analysis). In *Campbell*, this court detailed the interplay between Article I, section 9, and the Fourth Amendment:

> "We note that there is no presumption that interpretations of the Fourth Amendment by the Supreme Court of the United States are correct interpretations of Article I, section 9. *See State v. Kennedy*, 295 Or 260, 265–67, 666 P2d 1316 (1983); *State v. Caraher*, 293 Or 741, 748–52, 653 P2d 942 (1982). Article I, section 9, and the Fourth Amendment have a common source in the early state constitutions, but they have textual and substantive differences. Even were the provisions identical, this court would nonetheless be responsible for interpreting the state provision independently, though not necessarily differently. Majority opinions of the Supreme Court of the United States may be persuasive, but so may concurring and dissenting opinions of that court, opinions of other courts construing similar constitutional provisions, or opinions of legal commentators. What is persuasive is the reasoning, not the fact that the opinion reaches a particular result."

306 Or at 164 n 7. *See also Caraher*, 293 Or at 750 ("There have been recurring reminders from members of this court that we remain free * * * to interpret our own constitutional provision regarding search and seizure and to impose higher standards on searches and seizures under our own constitution than are required by the federal constitution. This is part of a state court's duty of independent constitutional analysis.").

The two strains of law interpreting both constitutional provisions deal in similar concepts and there are naturally points of convergence between the Fourth Amendment and Article I, section 9. For example, both constitutional provisions protect privacy, and in interpreting both provisions courts look to social and legal norms to discern the contours of the privacy that is protected.

But Article I, section 9, provides a stouter, less variable degree of privacy protection than the Fourth Amendment. This court should approach bank records under Article I, section 9, in accordance with that vigorous protection rather than continuing to rely on the Fourth-Amendment-oriented doctrine that the *Johnson* court, and the Court of Appeals in relying on *Johnson*,[19] seem to have adopted.

The chief difference between Article I, section 9, and the Fourth Amendment in the context of personal privacy is, of course, that section 9 protects the privacy to which the people of Oregon objectively have a *right*, *Campbell*, 306 Or at 164, while the Fourth Amendment protects only that privacy which a person subjectively expects and which society is prepared to recognize as reasonable. *Katz*, 389 US at 361 (Harlan, J., concurring).

Under the Fourth Amendment, third party records are unprotected. Because a person voluntarily "reveal[s] his affairs" to a phone company or a bank or other such entity, the person assumes the risk that information about

---

[19] *See State v. Ghim*, 267 Or App 435; *State v. Sparks*, 267 Or App 181, 340 P3d 688, *rev den* 375 Or 325 (2015) (no privacy interest in utility company records); *State v. Delp*, 218 Or App 17, 178 P3d 259, *rev den* 345 Or 317 (2008) (no privacy interest in non-content internet service provider records); *State v. Magana*, 212 Or App 553, 159 P3d 1163, *rev den* 343 Or 363 (2007) (no privacy interest in cellular telephone call records). The Court of Appeals decision in *State v. Gonzalez*, 120 Or App 249, 852 P2d 851, *rev den* 318 Or 61 (1993), shares the Fourth Amendment hallmark of these post-*Johnson* cases, but was issued before this court decided *Johnson*.

those affairs will in turn be revealed to the government, and therefore has no reasonable expectation of privacy in the information. *Miller*, 425 US at 443. In addition, the Court held that the bank records at issue in that case were the bank's business records, not the defendant's private papers, and that the defendant had no privacy interest in the content of checks, deposit slips, etc., because those items were not confidential communications. *Id.* at 440-43. In *Smith*, the Court held that the warrantless installation and use of a pen register on the defendant's telephone line was not a search because, under *Miller*, any expectation of privacy that the defendant may have had in the numbers that he dialed on his telephone (thereby providing them voluntarily to a third party, the telephone company) was not "legitimate." *Smith*, 442 US at 744.

But recent Supreme Court case law raises doubts about the continuing viability of the third party doctrine under *Miller* and *Smith*. In her concurrence in *United States v. Jones*, a case that dealt with GPS surveillance by means of a transmitter attached to the defendant's car, Justice Sotomayor expressed concerns with a doctrine that has not evolved along with the technological and organizational developments of the last four decades:

> "* * * [T]he same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations. Under that rubric, * * * at the very least, longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.

> "In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. * * * . The Government can store such records and efficiently mine them for information years into the future. * * *. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices * * *.
>
> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society."

Jones, 132 S. Ct. 945, 955-56, 181 L. Ed. 2d 911 (2012) (Sotomayor, J., concurring) (internal quotation marks and citations omitted). Justice Sotomayor wrote specifically of GPS surveillance in her opinion, but many of the same concerns are relevant to largely unfettered government access to the kind of information at issue here.

In *Riley v. California*, ___ US ___, 134 S Ct 2473, 189 L Ed 2d, (2014), the majority showed similar uneasiness with respect to government access to the content of cellular telephones, noting in particular that unrestricted access to cell phones exposed, in effect, a person's whole life to state view, including, potentially, "every bank statement from the last five years." *Riley*, 134 S Ct at

2493. The Court has yet to decide a third party records case in "the modern era in which social norms and technologies dictate that vastly more personal information resides with third parties." Henderson¸ *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 Iowa L Rev at 42.

The Supreme Court appears to be moving gradually away from the bright-line third party records doctrine set forth in its 1970s cases. This court, too, should move away from that approach by rejecting the *Johnson/Miller/Smith* approach to third party records.

CONCLUSION

For the foregoing reasons, petitioner respectfully asks this court to reverse the decision of the Court of Appeals and remand his case to the trial court for further proceedings.

Respectfully submitted,

ERNEST G. LANNET
CHIEF DEFENDER
CRIMINAL APPELLATE SECTION
OFFICE OF PUBLIC DEFENSE SERVICES

ESigned

MORGEN E. DANIELS OSB #075739
DEPUTY PUBLIC DEFENDER
Morgen.E.Daniels@opds.state.or.us

Attorneys for Defendant-Appellant
Denny D. Ghim

CERTIFICATE OF COMPLIANCE WITH ORAP 5.05(2)(d)

Petition length

I certify that (1) this petition complies with the word-count limitation in ORAP 5.05(2)(b) and (1) the word-count of this petition (as described in ORAP 5.05(2)(a)) is 11,138 words.

Type size

I certify that the size of the type in this brief is not smaller than 14 point for both the text of the petition and footnotes as required by ORAP 5.05(4)(f).

NOTICE OF FILING AND PROOF OF SERVICE

I certify that I directed the original Petitioner's Brief on the Merits to be filed with the Appellate Court Administrator, Appellate Courts Records Section, 1163 State Street, Salem, Oregon 97301, on July 14, 2015.

I further certify that, upon receipt of the confirmation email stating that the document has been accepted by the eFiling system, this Petitioner's Brief on the Merits will be eServed pursuant to ORAP 16.45 (regarding electronic service on registered eFilers) on Robert M. Wilsey, #085116, Assistant Attorney General, attorney for Respondent on Review.

Respectfully submitted,

ERNEST G. LANNET
CHIEF DEFENDER
CRIMINAL APPELLATE SECTION
OFFICE OF PUBLIC DEFENSE SERVICES

ESigned

_____

MORGEN E. DANIELS OSB #075739
DEPUTY PUBLIC DEFENDER
Morgen.E.Daniels@opds.state.or.us

Attorneys for Petitioner on Review
Denny D. Ghim