Ushering in a New Era: Assessing the Reasonable Expectation of Privacy vis-à-vis Cryptocurrency and Blockchain Data

NOAH LESIUK*

ABSTRACT

In recent years, the technology of cryptocurrency has become increasingly mainstream and has been documented as playing a role in the commission of contemporary criminal activity. The law must be responsive to these new techniques for committing crimes and adapt accordingly. Currently, there is a dearth of both jurisprudence and literature as it relates to section 8 of the *Canadian Charter of Rights and Freedoms* and the search and seizure of cryptocurrency by law enforcement. For the protections of section 8 to apply, there must be a reasonable expectation of privacy in the matter searched or seized by authorities. This paper analyzes the reasonable expectation of privacy as it relates to cryptocurrency in three different ways: first, in cryptocurrency transaction data on the blockchain, which is a public ledger that records cryptocurrency transactions; second, in various types of cryptocurrency storage mediums; and third, in user information on cryptocurrency exchanges. Previous section 8 *Charter* jurisprudence, U.S. case law, secondary sources, and blockchain data were all utilized to guide these analyses. Applying the reasonable expectation of privacy test to these inquiries yielded three distinct findings. It was determined that there is no reasonable expectation of privacy in cryptocurrency transaction data on the blockchain, that there is a reasonable expectation of privacy in various types of cryptocurrency storage mediums, and that there is a reasonable but

* Noah Lesiuk is a third-year law student at Robson Hall. He obtained his Bachelor of Arts degree in Criminal Justice from the University of Winnipeg in 2021 and wishes to pursue a carrer focused on the practice of Criminal Law. He would like to thank Professor John Burchill, the editors and peer reviewers of the Manitoba Law Journal, and his mother, Katina Andranistakis, for their support and guidance in the creation of this paper.

diminished expectation of privacy in user information on cryptocurrency exchanges.

Keywords: Cryptocurrency; Crypto; Blockchain; Search; Reasonable Expectation of Privacy; Privacy Interest.

I. INTRODUCTION

Fifteen years ago, on the heels of the 2008 financial collapse, an alias known as Satoshi Nakamoto developed Bitcoin, the first decentralized cryptocurrency, and authored a white paper explaining Bitcoin's revolutionary applications.[1] While the concept of cryptocurrency may have been esoteric and futuristic in 2008, one cannot deny that cryptocurrency has quickly penetrated the mainstream. Indeed, recent media coverage of crypto-related events has been plentiful.[2] While abundant, such news has been relatively negative, painting a less-than-satisfactory picture of cryptocurrency for potential investors.[3] Notably, in November 2022, the multi-billion-dollar crypto exchange, FTX, went insolvent, millions in customer assets were lost, and the CEO at the time now faces U.S. Securities and Exchange Commission ("SEC") charges for defrauding investors.[4] In a similar vein, notable celebrities such as Kim Kardashian have been charged by the SEC for unlawfully touting cryptocurrency to investors.[5] Contemporary companies have also been receptive to crypto;

---

1 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), online (pdf): *Bitcoin* <bitcoin.org/en/> [perma.cc/C6ZJ-9QDP] [Nakamoto].

2 See e.g., Don Pittis, "Crypto markets tumble and investors get their fingers burned" (13 May 2022), online: *CBC* <www.cbc.ca/news/business/crpto-tumble-column-don-pittis-1.6450411> [perma.cc/P8RP-7KUY]; Allison Morrow, "Crypto is joining the grown-up table, and no one is happy about it" (14 February 2023), online: *CNN* <www.cnn.com/2023/02/14/business/nightcap-crypto-regulation/index.html> [perma.cc/A3UA-YSM3].

3 See e.g., Jon Sarlin, "Stablecoins were supposed to be 'stable.' Then the crash came" (17 May 2022), online: *CNN* <www.cnn.com/2022/05/17/investing/luna-terra-losses-crypto-traders/index.html> [perma.cc/X38Q-UQBU]; Pete Evans, "Crypto market crashes anew as trading platform Celsius freezes up" (13 June 2022), online: *CBC* <www.cbc.ca/news/business/markets-crypto-monday-1.6486635> [perma.cc/33XC-38KP].

4 See *Securities and Exchange Commission v Samuel Bankman-Fried*, No 1:22-cv-10501 (SDNY 2022). See also Pete Evans, "Crypto trading platform FTX collapses into bankruptcy, dragging bitcoin price down with it" (11 November 2022), online: *CBC* < www.cbc.ca/news/business/ftx-bankrupt-friday-1.6648872> [perma.cc/X7RE-H6G5].

5 See "SEC Charges Kim Kardashian for Unlawfully Touting Crypto Security" (3 October 2022), online: *US Securities and Exchange Commission*

large companies such as Microsoft and payment processors such as PayPal have begun to accept cryptocurrency as a method of payment.[6] What can be discerned from the news surrounding cryptocurrency and its adoption by major corporations is simple: crypto's popularity is on the rise amongst the masses.

As a matter of pure logic, the more prevalent new technologies become, the more likely they are to be used in the commission of modern crime. The relationship between cryptocurrency and crime has been documented as "on the rise because cryptocurrencies are increasingly accepted as payments for online transactions of illegal commodities."[7] Indeed, crypto has created the opportunity for drug trafficking,[8] Ponzi schemes,[9] and money laundering.[10] The reason crypto proves useful for such illicit activities is due to the anonymity of its use. For instance, when making a crypto transaction, it is only documented as between crypto wallet addresses which are comprised of a string of random numbers and letters separated from the wallet user's identity.[11] With such a capacity for supporting criminal enterprise, it is self-evident that modern-day law enforcement must be responsive to the technologically advanced nature of cryptocurrency. As recognized by Justice Karakatsanis in *R v Fearon,* "as technology changes, our law must also evolve."[12] However, the law as it relates to the search and seizure of cryptocurrency by law enforcement has remained unaddressed. Such an untapped opportunity allows for the consideration of a novel issue vis-à-vis digital privacy and s. 8 of the *Canadian Charter of Rights and Freedoms*.[13] This paper seeks to address where the jurisprudence is lacking by assessing how the reasonable expectation of privacy applies to cryptocurrency transaction data on the blockchain, different methods for

---

<www.sec.gov/news/press-release/2022-183> [perma.cc/Q2SJ-KWZY].

6 See Sesha Kethineni & Ying Cao, "The Rise in Popularity of Crypto currency and Associated Criminal Activity" (2020) 30:3 Intl Crim Justice Rev 325 at 325 [Kethineni].

7 *Ibid* at 329.

8 See generally Marie Claire Van Hout & Tim Bingham, "'Silk Road,' the virtual drug marketplace: A single case study of user experiences" (2013) 24:5 Intl J Drug Policy 385. The Silk Road was an online drug marketplace where buyers utilized bitcoin to purchase narcotics online.

9 See *Securities and Exchange Commission v Trendon T Shavers and Bitcoin Savings and Trust*, 4:13-CV-416 (RC) (ALM) 1031 (ED Tex 2014).

10 See Kethineni, *supra* note 6 at 326-327.

11 An example is 34xp4vRoCGJym3xR7yCVPFHoCNxv4Twseo. This is Binance's (the largest cryptocurrency exchange) wallet address on the Bitcoin blockchain, meaning only Bitcoin can be sent and received from this address.

12 *R v Fearon,* 2014 SCC 77 at para 102 [*Fearon*].

13 See *Canadian Charter of Rights and Freedoms,* s 8, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

storing cryptocurrency, and user information on cryptocurrency exchanges. Principally, it shall be contended that there is no reasonable expectation of privacy in cryptocurrency transaction data on the blockchain, that there is a reasonable expectation of privacy in various types of cryptocurrency storage mediums, and that there is a diminished reasonable expectation of privacy in user information on cryptocurrency exchanges.

To advance these arguments, the following five-part structure shall be implemented. First, a brief explanation of cryptocurrency and the blockchain will be provided to bestow the reader with sufficient knowledge so they may better understand these concepts. Second, the s. 8 *Charter* jurisprudence as it relates to the reasonable expectation of privacy will be summarized with a specific focus on informational privacy. Third, the reasonable expectation of privacy in cryptocurrency transaction data itself will be assessed. The decentralized nature of such data, which is available for all to see on the public blockchain, will be deemed a factor seriously impeding any reasonable expectation of privacy. Fourth, the reasonable expectation of privacy in various mediums for storing cryptocurrency will be assessed. This analysis will concentrate on three types of storage, in particular, those being mobile, desktop, and hardware wallets. It will be contended that all three forms of storage likely attract a reasonable expectation of privacy. While it should be noted that there are other forms of storage, assessing every medium of doing so is beyond the cursory scope of this paper. As such, those deemed most relevant and contentious about s. 8 were chosen for analysis. Lastly, the reasonable expectation of privacy in an individual's user information on cryptocurrency exchanges will be examined. The purview such information can provide into the intimate details of one's financial preferences and choices, paired with considerations of control and third-party confidentiality, will be evaluated in determining why a diminished reasonable expectation of privacy attaches to this information.

II. Cryptocurrency and the Blockchain: A Basic Overview

To better understand the forthcoming aspects of this paper, it is first necessary to provide a simple explanation of cryptocurrency and the blockchain. Irrespective of the mainstream nature of crypto, its basic premises and functions still require a degree of elucidation to enhance general comprehension as it pertains to the topic.

The inception of cryptocurrency is often attributed to the Bitcoin whitepaper authored by an alias known as Satoshi Nakamoto in 2008.[14] Released following the 2008 Global Financial Crisis, which caused a significant amount of the public to lose trust in modern financial institutions,[15] cryptocurrency was envisioned as a digital-based transaction system which removed the centralized authority of financial institutions from transactions.[16] Although Nakamoto's whitepaper was based solely on Bitcoin, its contents equally explain cryptocurrency as a concept. In its most simple form, Bitcoin, and thus cryptocurrency in general, was explained by Nakamoto as a "purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution."[17] Premised on the issues of trust-based systems which require a third-party financial institution to serve as a medium to effect financial transactions, crypto was seen as a solution to attenuate the risks in a trust-based process. By removing the third-party intermediary, cryptocurrency is not controlled by any financial institution or government and is secured by the underlying technology of cryptography, which essentially makes it impossible to counterfeit.[18] On a basic level, cryptography is a secured communications technique associated with mathematical algorithms that ensure communication between parties is authentic, unaltered, and private.[19] Further, in normal financial transactions, every party and institution involved must keep their records of the transaction. This presents risks of possible *post hoc* modification of records as nothing prevents the parties from doing so.[20] However, cryptocurrency mitigates this risk by operating on a blockchain, which is essentially a ledger that contains a public record of all cryptocurrency

---

14 See Francisco Javier Garcia Corral et al, "A Bibliometric Review of Cryptocurrencies: How Have they Grown?" (2022) 8:2 Financial Innovation 1 at 2 [Garcia Corral]. See also Nakamoto, *supra* note 1.

15 See generally Felix Roth, "The Effect of the Financial Crisis on Systemic Trust" (2009) 44:4 Intereconomics 203; Timothy Earle, "Trust, Confidence, and the 2008 Global Financial Crisis" (2009) 29:6 Risk Analysis 785. The Global Financial Crisis of 2008 resulted from a culmination of factors such as extreme risk taking by global financial institutions, predatory lending, and the bursting of the U.S. housing market bubble.

16 See Nakamoto, *supra* note 1 at 1.

17 *Ibid.*

18 See Mary C Lacity, "Crypto and Blockchain Fundamentals" (2020) 73:2 Ark L Rev 363 at 367 [Lacity].

19 See Greg S Sergienko, "Self Incrimination and Cryptographic Keys" (Updated version 16 March 2023), online: *Gary Kessler Associates* <www.garykessler.net/library/crypto.html> [perma.cc/2GZU-VLJP].

20 See Lacity, *supra* note 18 at 365-366.

transactions made on that blockchain.[21] For example, Bitcoin operates on the Bitcoin blockchain. Any and every transaction involving Bitcoin is recorded on that blockchain as a public record that anyone with access to the internet can see.[22] The blockchain addresses the possible risk of altered records in traditional financial transactions as it is immutable, transaction records cannot be changed or deleted, and records become permanently documented.[23] While users transacting on a blockchain can enhance the security of their transactions by utilizing a Virtual Personal Network (VPN) to encrypt their data, disguise their IP address, and hide their location,[24] the transaction data itself is still fully recorded on the blockchain and remains unaltered. Although a VPN generally enhances the security and anonymity of an internet user, it cannot manipulate the data recorded on the blockchain. Ultimately, a blockchain is an unalterable public ledger of cryptocurrency transactions and serves as a "universal record of truth."[25]

The records kept on a blockchain show the transactions between cryptocurrency wallet addresses but do not reveal the personal information of the individuals or institutions making those transactions.[26] For instance, if party A utilized Bitcoin to buy an item from party B, then the blockchain transaction data would show the Bitcoin wallet address of party A sending the Bitcoin to the Bitcoin wallet address of party B. The following example illustrates a recorded transaction on the Bitcoin blockchain which was simply located by accessing the public website Blockchain.com.[27]

---

21 See David Challenger et al, "Blockchain Basics and Suitability: A Primer for Program Managers" (2019) 30:3 J of Information Technology Management 33 at 37 [Challenger].

22 See Lacity, *supra* note 18 at 370.

23 See Challenger, *supra* note 21 at 37.

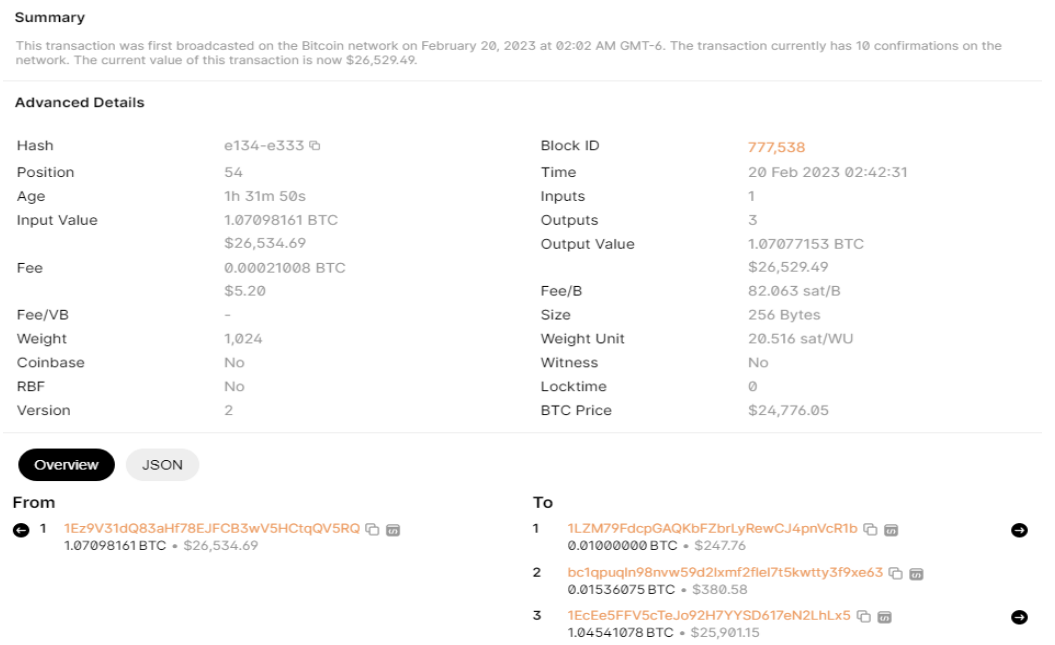
24 Chamandeep Kaur & Yogesh Kumar Sharma, "The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World" (2020) 8:6 International Journal of Recent Technology and Engineering 2336 at 2336-2337.

25 See Lacity, *supra* note 18 at 369.

26 *Ibid* at 370.

27 Blockchain.com, (Transaction created 20 February 2022), online: *Blockchain.com* <www.blockchain.com/explorer/transactions/btc/e1346a7eb498a875842d25f3f28f83bf4894e2a9d181545bd1db293f97e3e333> [perma.cc/6G8T-LZYW]. It should be noted that the provided example was a random transaction selected by the author and the author is in no way affiliated with any of the four Bitcoin wallet addresses contained in the photograph.

Figure 1: Public Bitcoin Blockchain Transaction Data



As can be seen, the blockchain transaction data shows that the Bitcoin wallet address on the left sent $26,534.69 USD worth of Bitcoin to three different Bitcoin wallet addresses. This not only shows how much USD and Bitcoin were sent but also the exact time and date of the transaction along with all the wallet addresses involved. Evidently, the blockchain records crypto transactions in a rather comprehensive and easy-to-understand manner for the public to view.

When the cryptocurrency changes and is on a different blockchain, such as the coin Ethereum which operates on the Ethereum blockchain, the wallet address will be different than the wallet address for Bitcoin. In effect, this means that an actual cryptocurrency wallet utilized to store crypto, such as a physical ledger or an app on one's computer or cellular device, has distinct sub-addresses for each of the different blockchains that cryptocurrencies operate on.[28] The different ways of storing cryptocurrency will be explored later in this paper, but generally, there are two ways of

[28] See Bitpay, "Crypto Wallet Addresses: What They Are and How to Create One" (2 February 2023), online: *Bitpay* <bitpay.com/blog/crypto-wallet-addresses/> [perma.cc/S839-C7TJ]; *United States of America v Ellingson*, 2023 BCSC 124 at para 17 [*Ellingson*].

doing so: either on a "cold" wallet, which is an offline wallet such as a hardware ledger, or on a "hot" wallet, which is an online wallet such as an app on one's desktop or mobile phone.[29] It is important to note that cryptocurrency exchanges also offer users a wallet to utilize both inside and outside the confines of that exchange.[30]

Overall, cryptocurrency is a form of decentralized currency. As aforementioned, cryptocurrency transactions do not require a central authority to act as an intermediary and all transactions are publicly recorded on the blockchain for anyone to browse. Thus far, crypto has remained relatively unregulated although it has become increasingly incorporated into the mainstream as a method of payment processing, data recording, and transacting.[31] This lack of regulation, paired with what has been called cryptocurrency's "simplicity of use," has been deemed to contribute to why it is utilized in criminal activities.[32] With this in mind, how law enforcement in Canada will go about conducting searches and seizures of cryptocurrency is a serious consideration. An even more salient question is if, and when, such searches would attract the protection of s.8 of the *Charter,* which guarantees the right to be free from unreasonable search and seizure.[33] Now that a basic explanation of cryptocurrency and the blockchain has been provided, it is apt to shift focus and scrutinize these concepts in light of s.8 of the *Charter* and its surrounding jurisprudence. However, it will first prove useful to review the operation of s. 8 of the *Charter* and its development over time.

III. Section 8 and The Reasonable Expectation of Privacy: A Review

In 1984, the Supreme Court of Canada's ("SCC") seminal case on s. 8 of the *Charter*, *Hunter v Southam,* required the SCC to interpret s.8 of the *Charter* and its breadth for the first time.[34] Writing for a unanimous court, Justice Dickson found that s. 8 of the *Charter* "protects people, not places"

---

29 Judith N'Gumah, "Evaluating Security in Cryptocurrency Wallets" (2021) 115 Culminating Projects in Information Assurance 1 at 9 [N'Gumah].

30 See *Ellingson*, *supra* note 28 at paras 25-28.

31 See Tina van der Linden & Tina Shirazi, "Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?" (2023) 9:22 Financial Innovation 1 at 2.

32 Garcia Corral, *supra* note 14 at 5.

33 See *Canadian Charter of Rights and Freedoms,* s 8, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

34 See *Hunter et al v Southam inc*, [1984] 2 SCR 145 [*Hunter*].

and guarantees the right to be free from unreasonable search and seizure.[35] This guarantee was deemed to trigger only if an individual had a reasonable expectation of privacy in the subject matter searched. Thus, the threshold question for whether s.8 of the *Charter* applies is whether the individual had a reasonable expectation of privacy in the subject matter that was searched or seized. [36] Elaborating on how such a determination is to be made, Justice Dickson held that an assessment would be required. Namely, balancing the public's interest in being left alone from government intervention with the government's interest in infringing on an individual's privacy in the name of crime control.[37] Only once this threshold test is met will a court then proceed to determine whether the impugned search or seizure was conducted in a reasonable manner compliant with s.8 of the *Charter*.[38] Seeing as this paper only seeks to explore the reasonable expectation of privacy vis-à-vis cryptocurrency, this threshold portion of the s. 8 test will form the crux of its analyses moving forward.

Eventually, the SCC would go on to add further clarity to the reasonable expectation of privacy threshold in *R v Edwards*.[39] In *Edwards*, the SCC held that a reasonable expectation of privacy is to be determined based on the "totality of the circumstances" and laid out a non-exhaustive list of factors to be considered in this evaluation.[40] The SCC would eventually move on to streamline this assessment in *R v Tessling* and adjust the threshold test into four separate prongs.[41] This would be refined to some degree years later in *R v Patrick* and the following test, confirmed numerous times throughout the jurisprudence, remains the present-day totality of the circumstances test for whether there is a reasonable expectation of privacy:

> (1) What was the subject matter of the alleged search?
> (2) Did the claimant have a direct interest in the subject matter?
> (3) Did the claimant have a subjective expectation of privacy in the subject matter?
> (4) If so, is this subjective expectation of privacy objectively reasonable,

---

35 *Ibid* at para 159.

36 See Richard Jochelson & David Ireland, *Privacy in Peril: Hunter v Southam and the Drift from Reasonable Search Protection* (Vancouver: UBC Press, 2019) at 24.

37 See *Hunter*, *supra* note 34 at paras 159-160.

38 See *R v Edwards*, [1996] 1 SCR 128 at para 45 [*Edwards*]; *R v Cole*, 2012 SCC 52 at para 36 [*Cole*]; *R v Reeves*, 2018 SCC 56 at para 14; *R v Wise*, [1992] 1 SCR 527 at 533.

39 See *Edwards*, *supra* note 38.

40 *Ibid* at para 45.

41 See *R v Tessling*, 2004 SCC 67 at para 32 [*Tessling*].

> having regard to the totality of the circumstances?[42]

If the answer to the fourth part of the inquiry is yes, this being that the claimant's subjective expectation of privacy was objectively reasonable, then the claimant will have the required standing to advance a section 8 claim as their reasonable expectation of privacy is made out.[43]

In assessing the first part of the test, the subject matter being searched must not be construed too narrowly. It must be determined by considering the nature of the privacy interests which are potentially infringed upon by the state action and what information may be revealed by such state action.[44] The three different types of privacy interests are personal privacy, territorial privacy, and informational privacy. While the subject matter of a search generally falls within one of these three categories, it is important to note that they may overlap.[45] For this paper, informational privacy forms the most salient of these categories and will be the root of focus from here on out. Informational privacy has been held to represent "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[46] Essentially, informational privacy is underpinned by the values of dignity, integrity, and autonomy, and involves information that an individual would want to shield from the state as it may reveal intimate details of their lifestyle and personal choices.[47] When characterizing the subject matter of an informational privacy-based search, the information that data can reveal, and the direct and immediate inferences that can be drawn from it, must be taken into account.[48] Ultimately, the ethos of informational privacy is the protection of a biographical core of personal information that an individual would wish to control and not have peered into by the state.[49]

---

42 *Ibid*; *R v Patrick*, 2009 SCC 17 at para 27 [*Patrick*]; *Cole, supra* note 38 at para 40; *R v Spencer,* 2014 SCC 43 at para 12 [*Spencer*]; *R v Jones*, 2017 SCC 60 at para 13 [*Jones*]; *R v Marakah*, 2017 SCC 59 at para 11 [*Marakah*]. See also David Ireland & Richard Jochelson "The Reasonable Expectation of Privacy: Digital Interests in the Supreme Court of Canada in Section 8 Jurisprudence (2010-2020)" in Christopher DL Hunt & Robert Diab, eds, *The Last Frontier: Digital Privacy and the Charter* (Toronto: Thompson Reuters, 2021) at 7.

43 See *Tessling*, *supra* note 41 at para 33.

44 See *Spencer*, *supra* note 42 at paras 26, 31.

45 See *Tessling, supra* note 41 at para 20. See also *R v Gomboc*, 2010 SCC 55 at para 19 [*Gomboc*].

46 *Ibid* at para 23 quoting, Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1970).

47 See *R v Plant*, [1993] 3 SCR 281 at 293 [*Plant*].

48 See *Spencer, supra* note 42 at para 31; *Marakah*, *supra* note 42 at paras 14, 16.

49 *Ibid* at para 27.

In *R v Spencer*, the SCC held that informational privacy is composed of three conceptually different understandings of privacy: privacy as anonymity, privacy as secrecy, and privacy as control.[50] Privacy as secrecy relates to the concept that there is a reasonable expectation information that is disclosed in confidence will be held accordingly in trust and confidence by the entity or person to whom that information is disclosed.[51] Privacy as control signifies the idea that individuals have control over their information such that they can determine what information about them is to be communicated with others.[52] Lastly, privacy as anonymity allows "individuals to act in public places but to preserve freedom from identification and surveillance."[53] These concepts will go on to play a minor role in the forthcoming analyses as they relate to informational privacy and cryptocurrency.

Concerning the second portion of the totality of the circumstances test, it is not particularly difficult to satisfy. For an individual to have a direct privacy interest in the subject matter searched, an individual must simply show that they had some degree of personal privacy interest in that subject matter.[54] The third portion of the totality of the circumstances test, which is whether the claimant had a subjective expectation of privacy in the subject matter searched, is also not a difficult standard to meet. As the court noted in *Patrick*, this stage of the test simply questions whether a claimant had, or can be presumed to have had, an expectation of privacy in the subject matter searched.[55] It is "not a high hurdle" to satisfy and is not focused on the reasonableness of such a belief.[56] Rather, reasonableness is assessed at the fourth stage of the test as the claimant's subjective expectation of privacy must be shown to be objectively reasonable.

Determining the objective reasonableness of a claimant's subjective expectation of privacy involves a contextual analysis which takes into consideration a variety of different factors. Over the years, the SCC has provided a variety of non-exhaustive considerations to be assessed in this inquiry. These include, but are not limited to:

> (a) The place where the search occurred;
> (b) whether the subject matter searched was in public view;
> (c) whether the subject matter searched was abandoned;

---

50 *Ibid* at para 38.
51 *Ibid* at para 39.
52 *Ibid* at para 40; *R v Dyment*, [1988] 2 SCR 417 at 429.
53 *Ibid* at para 43.
54 See *Marakah*, *supra* note 42 at para 21; *Cole*, *supra* note 38 at para 43.
55 See *Patrick*, *supra* note 42 at para 36.
56 *Ibid*. See also *Jones*, *supra* note 42 at para 20.

> (d) whether the subject matter searched was already in the hands of third parties, and if so, whether it was subject to an obligation of confidentiality;
> (e) whether the police technique utilized was intrusive in relation to the privacy interest implicated;
> (f) whether the use of this police technique was itself objectively unreasonable;
> (g) whether the subject matter searched exposed any intimate details of the appellant's lifestyle, or information of a biographic nature;[57] and
> (h) other considerations such as control over the subject matter of the search and the context surrounding the search.[58]

These many factors, where relevant, are to be considered in the overall quantum of objective assessment. Although the analysis is inherently factual, the standard is normative rather than descriptive and is made from the "perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy."[59] The objective reasonableness portion of the reasonable expectation of privacy test is, as recognized by the SCC, often the battleground upon which the s 8 jurisprudence meets the most resistance.[60] The upcoming assessment of crypto-related searches and the reasonable expectation of privacy will necessarily face most of its tribulations in this metaphorical warzone.

With the legal aspects of s. 8 and the reasonable expectation of privacy now detailed, it is apt to apply this law to the various aspects of cryptocurrency that this paper seeks to explore. While the concept of cryptocurrency and the law is relatively recent and completely novel concerning s. 8 of the *Charter,* the arguments advanced will nevertheless be grounded in the s 8 jurisprudence.

IV. Problematically Public: The Reasonable Expectation of Privacy in Cryptocurrency Transaction Data on the Blockchain

Beginning the delve into cryptocurrency and the reasonable expectation of privacy, it is pragmatic to begin with transaction data contained on the blockchain as doing so sets the stage for the assessments that follow. As a brief refresher, blockchain transaction data refers to the

---

57 *Patrick, supra* note 42 at para 26.
58 *Marakah, supra* note 42 at para 38; *Cole, supra* note 38 at para 52.
59 *Patrick, supra* note 42 at para 14; *Spencer, supra* note 42 at para 18.
60 See *Tessling, supra* note 41 at para 43.

records kept on a blockchain that show the transactions between cryptocurrency wallet addresses. This information does not, however, reveal the personal details of the individuals or institutions making those transactions. Only their wallet addresses, the exact time the transaction was made, and the amount of cryptocurrency involved in the exchange are displayed.[61] For instance, in *R v Shaporov,* investigators utilized the blockchain to confirm the exact time the accused, who was already identified as the owner of a specific Bitcoin wallet address, conveyed Bitcoin to a website to access child pornography.[62]

At the forefront of establishing a reasonable expectation of privacy in cryptocurrency transaction data on the blockchain, it is first necessary to discern the subject matter of such a search. While the reasons why law enforcement may choose to look at this data may vary, the actual subject matter of the search, construed broadly with attention to possible inferences that can be drawn, leads to one general conclusion. This is because the subject matter of such a search is the electronic transaction data between two or more cryptocurrency wallet addresses. Whether law enforcement wishes to see what time a transaction was made, how much money was involved, which wallet addresses were implicated, and what cryptocurrencies were exchanged, this subject matter definition encapsulates all these possibilities. In this sense, the subject matter of the search is informational as it relates purely to data contained on the blockchain. This hypothesized subject matter description can be further supported by analogy. In *R v Marakah*, the majority held that the subject matter of the search of text message records was "the electronic conversation between two or more people."[63] Essentially, a search of crypto transaction data on the blockchain is similar, not in form, but in substance. Such a search involves looking at the records of an electronic transaction between two or more crypto wallet addresses. By adopting the shell of the *Marakah* majority's articulation, the subject matter proffered vis-à-vis cryptocurrency transaction data on the blockchain is both consonant with, and guided by, prior s. 8 jurisprudence. As such, this paper advances that the electronic transaction data between two or more cryptocurrency wallet addresses forms the subject matter of a search of cryptocurrency transaction data on the blockchain.

With the subject matter now defined, the other aspects of the reasonable expectation of privacy test must be explored. First, it is arguable that an individual has a direct interest in their electronic transaction data

---

61 See Lacity, *supra* note 18 at 370-371.

62 *R v Shaporov*, 2022 ONCJ 111 at para 78 [*Shaporov*].

63 *Marakah*, *supra* note 42 at para 19. See also *Jones, supra* note 42 at para 14.

on the blockchain as they utilized their crypto wallet to create such a transaction and, as a consequence, its data on the blockchain. That individual was a participant in, and an author of, that transaction.[64] This data can show when exactly that transaction was made, how much it was worth, and what other crypto wallet addresses were involved. It does not seem contentious to claim that an individual would have a direct interest in such information. For instance, if that individual engaged in a transaction with a crypto exchange, they may wish to go back and check that transaction to fill out their taxes.[65]

Turning to whether an individual would have a subjective expectation of privacy in their electronic transaction data on the blockchain, the answer is likely in the affirmative. As explained in *Patrick*, this is not a high hurdle to meet.[66] An individual could simply argue that they believed that their transaction data on the blockchain was private and would remain so. This is an especially prudent contention considering crypto is often touted as "generally anonymous."[67] Seeing as the subjective expectation of privacy is not particularly difficult to satisfy, it is more appropriate to assess whether this subjective expectation of privacy is objectively reasonable.

Assessing whether an expectation of privacy is objectively reasonable involves a variety of different considerations.[68] Beginning with the most basic, the place where the search would occur is on the blockchain as it stores the electronic transaction data between cryptocurrency wallet addresses. In *Tessling*, the SCC held that "a person can have no reasonable expectation of privacy in what he or she knowingly exposed to the public, or to a section of the public."[69] As previously mentioned, the blockchain acts as an unalterable public ledger that records crypto transactions made on that blockchain in a comprehensive and easy-to-understand manner. The blockchain's very purpose is to ensure transactions are permanently recorded and available for viewing by the public.[70] Anyone with access to the internet can search through these records and easily examine them through websites such as Blockchain.com.[71] This proves problematic for the

---

64 See *Marakah*, *supra* note 42 at para 21.

65 Cryptocurrencies are taxable in Canada. See Government of Canada, "Guide for cryptocurrency users and tax professionals" (26 June 2021), online: *Canada Revenue Agency* <www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency/cryptocurrency-guide.html>.

66 See *Patrick*, *supra* note 42 at para 37.

67 Garcia Corral, *supra* note 14 at 4.

68 See *Patrick*, *supra* note 42 at para 26.

69 *Tessling*, *supra* note 42 at para 40; *R v Stillmann*, [1997] 1 SCR 607 at para 62.

70 See Challenger, *supra* note 21 at 37.

71 See generally www.blockchain.com/explorer.

assertion that there is an objectively reasonable expectation of privacy in the electronic transaction data between crypto wallets. By utilizing cryptocurrency, the reasonable person knows, or ought to know, that the transactions they make are publicly recorded and available on the blockchain. Stated simply, it is unreasonable for there to be an expectation of privacy in inherently public information that anyone can access. While a counterargument may be mounted that it cannot be assumed that a reasonable person would be aware that their cryptocurrency transactions are publicly recorded, this contention falls short and attempts to utilize ignorance as a bastion. Irrespective of whether an individual is aware of the blockchain or not, this does not change the fact that the inherently public nature of the blockchain allows anyone with internet access to browse the records of cryptocurrency transactions. Further, how could it be objectively reasonable for a cryptocurrency user to be ignorant of the blockchain when it is quite literally the fundamental ethos of crypto?

It is also worth noting, as the Supreme Court of British Columbia in *United States of America v Ellingson* did, that the blockchain "only reflects the movement of funds between anonymous wallets and, therefore, cannot by itself be used to determine the identities of the persons involved in the transactions."[72] This is particularly important as it illustrates that blockchain transaction data itself maintains the anonymity of those implicated in the transaction. Consequently, such data alone cannot illustrate intimate details about one's life or biographical core of personal information as they remain anonymous under the guise of their crypto wallet address. Paired with the intrinsically public nature of the blockchain, this militates in favour of a finding that there is no objectively reasonable expectation of privacy.

United States jurisprudence has taken a similar approach. In *United States v Gratkowski*, at issue was whether Mr. Gratkowski had a reasonable expectation of privacy in his transaction information on the Bitcoin blockchain.[73] Finding that Mr. Gratkowski did not have such a privacy interest, the court held that "Bitcoin users are unlikely to expect that the information published on the Bitcoin blockchain will be private" and that "it is well known that each Bitcoin transaction is recorded in a publicly available blockchain."[74] The public nature of the blockchain was deemed to eviscerate any conception that there was a reasonable expectation of

---

72 *Ellingson*, *supra* note 28 at para 16.

73 *United States v Gratkowski*, 964 F.3d 3017 (5th Cir, 2020) at 1-2 [*Gratkowski*].

74 *Ibid* at 7.

privacy in transaction information on the blockchain.[75] This approach seems cogent and, as argued above, is the angle this paper has adopted.

As an added policy perspective, it would be impractical to consider looking at cryptocurrency transaction data on the blockchain as a search. If authorities had to obtain a warrant every time they wished to look at a crypto transaction on the blockchain, which is something any ordinary person could do without issue, this would unnecessarily constrain the crime-controlling capabilities of law enforcement. This notion is especially apt considering that a wallet address could be involved in thousands of transactions. If law enforcement was investigating a specific wallet address and it was involved in thousands of transactions with hundreds of other wallet addresses, it would seem unfeasible to require a warrant in each instance. The balance recognized in *Hunter v Southam* between the public's interest in privacy and the state intruding on this privacy in the name of effective crime control lends further credence to these contentions.[76] While the privacy interests of the public are minimal as blockchain transaction data itself reveals no details about the actual individuals involved, the crime-controlling capabilities of the state would be seriously hindered if they had to procure a warrant every time they wished to search this publicly available information. The impracticality of such a requirement, balanced against the minimal privacy interest in blockchain transaction data, militates in favour of ensuring the state is not unduly obstructed in combatting crime. Accordingly, it would be prudent to recognize that the browsing of such data does not amount to a search for the purposes of s. 8.

The inherently public nature of the blockchain and its maintenance of a crypto wallet user's anonymity without further information seriously hinders any notion that there is an objectively reasonable expectation of privacy in cryptocurrency transaction data on the blockchain. Anyone with access to the internet can browse through these records as they are open for public viewing and do not reveal who is making a transaction. On this basis, paired with similar thoughts echoed by United States jurisprudence, it is highly unlikely that there is a reasonable expectation of privacy in cryptocurrency transaction data on the blockchain. Consequently, such data likely does not attract the protections of s.8, nor does its inspection by authorities constitute a search under that section.

---

75 *Ibid* at 6-7.

76 *Hunter*, *supra* note 34 at paras 159-160.

V. MEDIUMS OF CRYPTOCURRENCY STORAGE AND THE REASONABLE EXPECTATION OF PRIVACY: DESKTOP, MOBILE, AND HARDWARE WALLETS

As aforementioned, cryptocurrency is stored in wallets. Unlike a traditional leather wallet, these wallets are mediums that allow a user to keep a balance of various cryptocurrencies and send or receive them accordingly.[77] There are two general ways of storing crypto: either in an online "hot" wallet or in an offline "cold" wallet.[78] Hot wallets are connected to the internet while cold wallets are akin to a safety deposit box holding one's crypto assets in a manner unconnected to the online world.[79] In particular, two types of hot wallets—desktop and mobile wallets–and one type of cold wallet—hardware wallets—will be discussed. Mobile wallets can be utilized via an app on one's cellular device and desktop wallets are an app or program on an individual's personal computer.[80] As can be discerned, these types of wallets are inherently found on, and connected to, an individual's personal devices such as a computer or mobile phone. On the other hand, hardware wallets are electronic devices, often USBs, that have programmed software to store crypto within them and act as a form of offline storage.[81] These wallets are seen as more secure than hot wallets as they are not connected to the internet and someone would need physical access to the hardware storage device to access the crypto on it.[82] With an explanation now provided concerning the basic functions of the types of crypto wallets that will be examined, it is apt to scrutinize them in light of s. 8 and the reasonable expectation of privacy.

Beginning with mobile and desktop wallets, it is pragmatic to assess them together. As recognized by Justice Cromwell in *R v Fearon*, cellular devices, especially smartphones, "are the functional equivalent of computers."[83] Approximately 84.4% of Canadians own a smartphone for personal use and, as such, any search of a crypto wallet on a mobile device is more than likely going to occur on a smartphone.[84] Turning to the

---

77 N'Gumah, *supra* note 29 at 7.

78 *Ibid* at 9.

79 Stevo Jokić et al, "Comparative Analysis of Cryptocurrency Wallets Vs Traditional Wallets" (2019) 65:3 ekonomika 65 at 67 [Jokić].

80 *Ibid* at 68.

81 *Ibid* at 69.

82 *Ibid.*

83 *Fearon, supra* note 12 at para 54.

84 Statistics Canada, "Smartphone personal use and selected smartphone habits by gender and age group" (6 June 2021), online: *Statistics Canada* <www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2210011501> [perma.cc/3NYD-

reasonable expectation of privacy analysis, the subject matter of a prospective search of these types of wallets must be determined. As explained by the majority in *R v Marakah*, the subject matter of a search must be described holistically and precisely without being confined to physical acts or spaces.[85] Although a search of mobile and desktop crypto wallets would necessarily take place on a personal computer or cellular device, it is not these devices nor their general contents that police would be after. Rather, the subject of the search would more than likely be the informational content on these cryptocurrency storage mediums. A similar articulation was offered by the SCC in *R v Cole* when a search of the data on an accused's laptop was being assessed.[86] The majority held that the subject matter of the search was the "data, or informational content of the laptop."[87] Analogously, a search of a cryptocurrency storage medium is to access its data, and thus, its informational content. While one may contend that such a construction of subject matter is confined to a physical space, that being a cryptocurrency storage medium, this fails to recognize that what authorities would be after is not the medium of storage itself, but the informational content it is storing. In this sense, the search is informational in scope and implicates privacy of control interests as it deprives the individual of the capacity to control whether or not the information searched is divulged to the state.[88] The informational content searched could include but is not limited to, the cryptocurrency assets held in the wallet, transaction data, and the wallet addresses for various blockchains.[89] Considering this, the subject matter for a search of a mobile and desktop crypto wallet can be characterized as the informational content contained on a cryptocurrency storage medium. This encapsulates the various forms of data contained in a cryptocurrency wallet while also ensuring that the subject matter is precisely defined. For clarity moving forward, it will be assumed that a searched mobile or desktop wallet is on an individual's personal device and their identity is known by authorities.

Turning to direct interest and subjective expectation of privacy in the subject matter, it is not difficult for a hypothetical claimant to establish both. It can easily be inferred that an individual has both a direct interest and subjective expectation of privacy in the informational content contained on their cryptocurrency storage medium. As previously

---

7VLH].

85 See *Marakah*, *supra* note 42 at paras 16-17.

86 See *Cole*, *supra* note 38 at para 41.

87 *Ibid*.

88 See *Spencer*, *supra* note 42 at para 40.

89 See Jokić, *supra* note 79 at 67-69.

mentioned, these cryptocurrency storage mediums store one's cryptocurrency assets, which are essentially personal financial assets. [90] Further, desktop and mobile wallets are themselves situated on personal electronic devices such as cell phones or computers. The SCC in both *Cole* and *R v Morelli* found that details of an individual's financial situation militate in favour of elevated privacy interests.[91] While this was done in the context of personal computers, it is equally applicable to cryptocurrency wallets as they illustrate an individual's financial details by revealing what crypto assets they hold, how much they hold, and how much those assets are worth. Such a purview into one's financial decisions and details surely attracts a direct interest and subjective expectation of privacy in the subject matter at hand.

As is often the case, determining whether this subjective expectation of privacy is objectively reasonable often proves to be the decisive factor. The SCC has recognized that characterizing the place of a search is difficult when it comes to electronic sources.[92] It is also worth considering whether the search for the informational content of a cryptocurrency storage medium is the search for a place itself or simply a thing. In *Marakah,* the SCC had to determine how electronic conversation data on a cellular device fit into the concept of a searched place and came up with two different possibilities.[93] The first possibility was that the electronic conversation did not occupy a specific physical area but the place of the search was an electronic "private chat room" existing in an electronic space.[94] The other possibility was that the place of the search was the device through which the messages were accessed or stored.[95] While not definitively determining the place, the court found that either possibility favoured a reasonable expectation of privacy. Seeing as the SCC only considered the electronic conversation data in terms of a place being searched and not a thing, this paper will do the same as it relates to the informational content of a cryptocurrency storage medium as it is also a form of electronic data.

Utilizing the two-pronged approach from *Marakah*, a similar construction of the place of the search can be crafted in terms of the informational content of a cryptocurrency storage medium. As the SCC in *Marakah* did when composing the first possibility, it is apt to analyze the

---

90 *Ibid* at 67-68.
91 See *Cole, supra* note 38 at para 47; *R v Morelli*, 2010 SCC 8 at para 103 [*Morelli*].
92 See *Marakah*, *supra* note 42 at para 51.
93 *Ibid* at paras 27-30.
94 *Ibid* at para 28.
95 *Ibid* at para 29.

informational content of a cryptocurrency storage medium in terms of electronic space. In the case of mobile and desktop crypto wallets, this informational content would be contained in an app or program. These mediums of storage essentially become a way to store, send, and receive crypto electronically, acting as one's vault of financial assets in a manner analogous to a bank account.[96] In this sense, these mediums of storage are effectively an electronic bank account for cryptocurrency ripe with information about transactions, blockchain wallet addresses, and held crypto assets. With this in mind, the place of a search for the informational content of a cryptocurrency storage medium can be construed as a bank account for cryptocurrency storage and transactions existing in an electronic space.[97] Accordingly, a reasonable person would presume that their bank account and its financial contents would remain highly private to that individual.

Another way in which to construe the place of the search is to adopt the second possibility offered in *Marakah*. As aforementioned, the SCC in *Marakah* found it a viable option to state that the place of the search of a text message conversation was the device through which the messages were accessed or stored.[98] Considering personal cellular devices and computers are the place through which law enforcement would access mobile and desktop crypto wallets, the logic from *Marakah* surely applies. Consequently, the place of the search for the informational content of a cryptocurrency storage medium can also be advanced as an individual's mobile phone or computer. On numerous occasions, the SCC has recognized a high privacy interest in these types of devices.[99] As such, it is certain that a reasonable person would have an expectation of privacy in their cellular device or computer.

In whichever manner the place of the search is articulated, similar to *Marakah*, both possibilities militate in favour of a reasonable expectation of privacy in the informational content of cryptocurrency storage mediums. Whether the place of the search is a bank account for cryptocurrency storage and transactions existing in an electronic space, or simply a cellular device or computer, both places denote areas in which an individual would undoubtedly have significant privacy interests.

An argument can be mounted against an objectively reasonable expectation of privacy on the basis that much of the informational content

---

96 See Jokić, *supra* note 79 at 67.

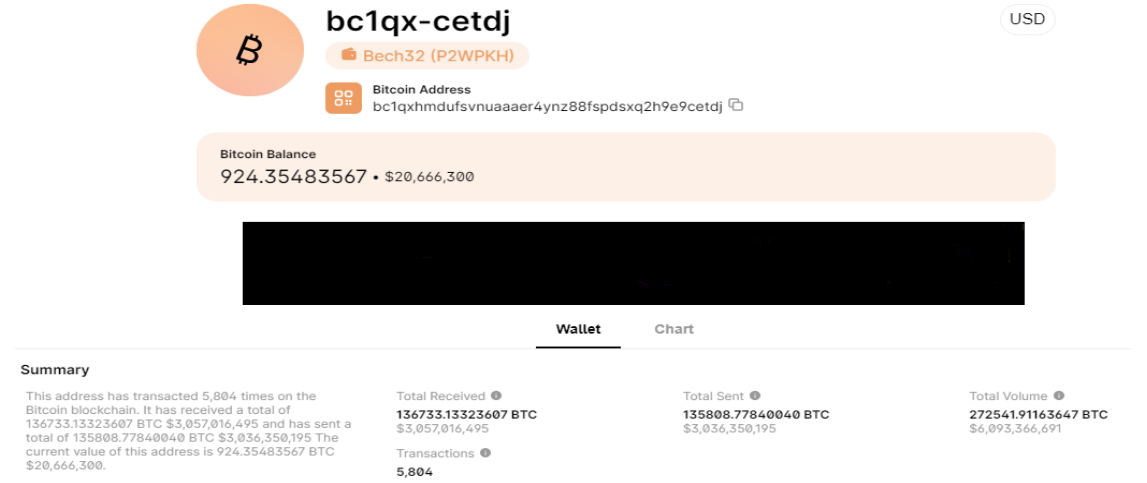
97 See *Marakah*, *supra* note 42 at para 28.

98 *Ibid* at para 29.

99 See *R v Vu*, 2013 SCC 60 at paras 24, 40-41; *Fearon*, *supra* note 12 at paras 51, 126; *Morelli*, *supra* note 91 at para 105; *Cole*, *supra* note 38 at para 3.

in a crypto wallet is publicly available. It was earlier illustrated how the public blockchain can show a crypto wallet address' transactions. Interestingly, other potentially sensitive information available for public viewing can also flow from a crypto wallet address if it is looked up on the blockchain. This includes the amount of cryptocurrency a wallet address contains on a certain cryptocurrency's blockchain, along with the amount of crypto that the wallet address has sent and received. For example, simply navigating blockchain.com and looking at a Bitcoin wallet address yields the information shown in the example below.[100]

Figure 2: Example Wallet Information on Blockchain



Although this data is sensitive, the individual behind the wallet address is still shrouded by the cloak of anonymity without further identifying information. However, if authorities search the informational content of a person's cryptocurrency storage medium, they can ascertain the crypto wallet addresses on it and attribute them to that individual. While the public availability argument is persuasive, it loses force when it is realized that without further information, this data, along with blockchain transaction data, still maintains the anonymity of the individual behind the guise of their wallet address. In juxtaposition, if authorities search the

100 Blockchain.com, (accessed 2 March 2022), online: *Blockchain.com* <www.blockchain.com/explorer/addresses/btc/bc1qxhmdufsvnuaaaer4ynz88fspdsxq2h9e9cetdj> [perma.cc/PP3C-HM7S].

informational content of a person's cryptocurrency storage medium on that person's personal device, they will almost always know who that individual is. Thus, the transaction data and crypto assets held are no longer anonymously hidden behind a wallet address but become attributed to that individual. This creates a conceptual difference. On one hand, the data by itself is publicly available but completely anonymous without further information. On the other, a search of one's crypto wallet on their personal device will connect that individual to that public data, rendering it no longer anonymous. Therefore, such a search implicates privacy interests, as it necessarily puts a name and identity to a crypto wallet address and thus the held crypto assets and transaction data flowing from it. In this sense, the data does not become publicly attached to an individual until police search their cryptocurrency storage device. This provides the information needed for law enforcement to create the link between an individual, their crypto assets, and their wallet transaction data, something the data on the blockchain cannot do in isolation. Ultimately, the public information contention must fail. While available publicly, it is only after authorities engage in an external search of the informational content of a cryptocurrency storage medium that the mask of anonymity is cast off this public data and linked to the individual. As the SCC in *R v Spencer* cogently stated when discussing anonymity and internet privacy, in "'public acts we do not expect to be personally identified and subject to extensive surveillance but seek to merge into the 'situational landscape.'"[101] In transacting on the public blockchain, an individual seeks to merge into that landscape. Searching the informational content of a crypto storage medium, allows the individual to be personally identified in this landscape, undermining their privacy in anonymity interests as a consequence.

Shifting to other considerations, the element of control is worth discussing. Control has been deemed a relevant factor in determining whether an expectation of privacy is objectively reasonable.[102] While important, the presence of control or the lack of, is not determinative of the reasonable expectation of privacy but factors into the overall assessment.[103] Undoubtedly, individuals exercise meaningful control over the informational content of their cryptocurrency storage mediums. Not only is such data contained on a personal device that an individual

---

101 *Spencer*, *supra* note 42 at para 44, quoting M Gutterman, "A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance" (1988) 39 *Syracuse L Rev* 647 at 706.

102 See *Edwards*, *supra* note 38 at para 45; *Cole*, *supra* note 38 at para 51; *Marakah*, *supra* note 42 at para 38.

103 See *R v Buhay*, 2003 SCC 30 at para 22.

possesses, thus exerting literal control over the contents of that device, but an individual can choose when, how, and to whom they disclose that this information is linked to them.[104] On this basis, the element of control seems to favour a reasonable expectation of privacy.

Finally, whether the informational content of cryptocurrency storage mediums tends to reveal "a biographical core of personal information" must be assessed.[105] As recognized by the SCC, this includes information which exposes the intimate details of one's lifestyle and personal choices.[106] A search of the informational content on a cryptocurrency storage medium allows authorities to have a glimpse into the details of one's financial holdings in terms of cryptocurrency. This reveals how much money an individual holds in crypto, what assets they personally hold and have previously held, and when and for how much they have made transactions with those assets. Such a search divulges to the state the personal choices and lifestyle of an individual by illustrating how they choose to spend their money along with when and how much of it they spend. Essentially, this provides a purview into the financial situation and preferences of an individual. As previously mentioned, the SCC has viewed an individual's financial situation as attracting a privacy interest.[107] The capacity of a search of the informational content of cryptocurrency storage mediums to expose an individual's financial preferences, holdings, and when and how they choose to spend their money, quite obviously uncovers the intimate details of one's personal choices and lifestyle. This being the case, the private information revealed by this type of search militates in favour of a reasonable expectation of privacy.

Taking into consideration the place of the search, control over the content searched, and the private and intimate details revealed by the search of the informational content on one's cryptocurrency storage medium, the expectation of privacy with such content can be deemed objectively reasonable. Accordingly, it can be claimed that there is a reasonable expectation of privacy in mobile and desktop crypto wallets.

In terms of hardware wallets, much of the same analysis can be adopted from the assessment of desktop and mobile wallets. The subject matter of a hardware wallet search is still the informational content contained in that cryptocurrency storage medium. Additionally, a search of a hardware wallet still provides a view into one's financial decisions and details, similarly attracting a direct interest and subjective expectation of privacy in the

104 See *Marakah*, *supra* note 42 at para 39.
105 *Plant*, *supra* note 47 at 293.
106 *Ibid.*
107 See *Cole*, *supra* note 38 at para 47; *Morelli*, *supra* note 91 at para 103.

subject matter. Whether this subjective expectation of privacy is objectively reasonable generally hinges on the same contentions. The place of the search is the medium of crypto storage, this being the hardware wallet, which also acts as an electronic bank account for cryptocurrency storage and transactions. One difference is that the place of the search can also be construed as the individual's personal hardware device itself, which is essentially a USB.[108] Either way, the search of someone's financial assets or personal USB device arguably favours a reasonable expectation of privacy. The argument pertaining to the public nature of the informational contents on the crypto storage device fails for the same reason it did for mobile and desktop wallets. It is only once police search an individual's hardware wallet that the public data on it becomes attached to that individual. Regarding control, an individual also exerts literal control over and possession of, the contents of the hardware wallet and can choose when, how, and to whom they disclose that the information on it relates to them. Lastly, a search of the informational content on a hardware wallet also divulges information about an individual's personal financial choices and lifestyle to the state. Namely, how much money an individual holds in crypto, what assets they personally hold and have previously held, and when and for how much they have made transactions with those assets. Based on all these factors, it can be concluded that there is also a reasonable expectation of privacy in hardware wallets.

The contentions advanced have strongly supported the claim that there is a reasonable expectation of privacy in mobile, desktop, and hardware crypto wallets. These devices are contained on or are personal devices themselves, and their informational content exposes intimate details relating to the owner's financial proclivities. If the state could peer into one's financial data with complete impunity, irrespective of how they do so, George Orwell's dystopian novel of mass surveillance, *1984,* does not seem so farfetched.[109]

VI. Creating a Connection between the Individual and the Wallet: User Information on

[108] See Jokić, *supra* note 79 at 69.

[109] See George Orwell, *Nineteen Eighty-Four* (London: Penguin Classics, 2021).

CRYPTOCURRENCY EXCHANGES AND THE REASONABLE EXPECTATION OF PRIVACY

Cryptocurrency exchanges are the main platforms that facilitate the trading of cryptocurrencies.[110] Exchanges often have a KYC or 'know your customer' policy to access their services. This policy requires a user to verify their identity with the exchange through means such as their government-issued ID.[111] It is also true that exchanges often give users crypto wallet addresses so they may send, receive, and transact crypto both on and outside that exchange.[112] This means that cryptocurrency exchanges have the personal information necessary to attach an identity to the wallet addresses that they provide to their users. These wallets can be used on the exchange platform but are not their own form of wallet. This is because they are still accessed via mobile devices or personal computers, essentially making them a type of hot wallet such as a mobile or desktop wallet. Moving forward, these will simply be called exchange wallet addresses for clarity.

In *Shaporov,* a Bitcoin wallet address from the exchange Coinbase was used on a website to buy child pornography.[113] The court noted that American authorities subpoenaed Coinbase and examined their records to determine the owner of that wallet address.[114] Through doing so, they were able to procure the information of the accused and connect him to that wallet address.[115] After passing this evidence off to Canadian authorities, it factored heavily into the accused's conviction for child pornography.[116] As can be seen, user information on a cryptocurrency exchange can prove useful for authorities, specifically when a wallet address they are investigating has been given to the user by a cryptocurrency exchange. Interestingly, this poses an issue similar to the one raised in *Spencer*, that being whether there was a reasonable expectation of privacy in subscriber information held by an internet service provider. In these circumstances,

---

110 See Pengcheng Xia et al, "Characterizing cryptocurrency exchange scams" (2020) 98 Computers & Security 1 at 1.

111 See Binance, "Important Changes About Binance Identity Verification" (20 August 2021), online: *Binance* <www.binance.com/en/support/announcement/important-changes-about-binance-identity-verification-51bf294e26324211a4731ca998e110ca> [perma.cc/92S3-3KSD]; Binance, "How to Complete Identity Verification" (22 April 2019), online: *Binance* <www.binance.com/en/support/faq/how-to-complete-identity-verification-360027287111> [perma.cc/C6UX-9CLK].

112 See *Ellingson*, *supra* note 28 at paras 25-28.

113 See *Shaporov, supra* note 62 at paras 1-5.

114 *Ibid* at para 6.

115 *Ibid* at paras 6-7, 299-303.

116 *Ibid* at paras 6-7.

the question is whether there is a reasonable expectation of privacy in user information held by a cryptocurrency exchange.

Beginning with the subject matter of the search, authorities would likely be seeking an exchange user's information so they may link the identity revealed by this information with an exchange wallet address. In *Spencer,* where police accessed an individual's subscriber information from an ISP, the court rejected the notion that the subject matter of the search was simply the name and address of the accused. Rather, they held that what the police were really after was the connection between this identifying information and what it tends to reveal about the accused's activity on the internet.[117] This seems to be analogous in the case of a search of user information on a crypto exchange as authorities will be looking to connect an individual's identity with a specific exchange wallet address. In this sense, it is logical to characterize the subject matter of a search for user information on a cryptocurrency exchange as the identity of a cryptocurrency exchange user in connection to a specific crypto wallet address. A search of this nature would be informational in scope as it seeks to reveal the identity behind an exchange crypto wallet address so the state may connect this individual with that wallet's underlying information, thereby implicating privacy of anonymity concerns.

Regarding direct interest and subjective expectation of privacy in the subject matter, a claimant could easily satisfy these requirements. Surely, a hypothetical claimant would have such an interest and expectation of privacy in information that can personally link them to a crypto wallet and the transaction data or assets of that wallet. An individual could simply argue that they believed their personal information would remain confidential and would not be shared by the cryptocurrency exchange. As was the case for blockchain data and cryptocurrency storage mediums, it is whether the reasonable expectation of privacy is objectively reasonable that proves most controversial.

To begin, it cannot be said that the subject matter of a search for user information on a cryptocurrency exchange is already in public view or abandoned. This identifying data is kept by an exchange, often under a privacy policy, and is not available for the public to simply browse.[118] Unless the exchange chooses to share such information, it will generally remain anonymous.

---

117 See *Spencer, supra* note 42 at paras 31-33.

118 See Binance, "Privacy Notice – Binance" (29 September 2022), online: *Binance* < www.binance.com/en/privacy> [perma.cc/48EK-U2UX].

A more salient consideration is whether the subject matter searched was already in the hands of third parties, and if so, whether it was subject to an obligation of confidentiality.[119] While United States jurisprudence was previously drawn upon to support the contention that there is no reasonable expectation of privacy in transaction data on the blockchain, no such harmony likely exists between Canada and the U.S. in terms of user information on cryptocurrency exchanges. Unlike the United States' third-party doctrine, which holds that a person generally has no legitimate expectation of privacy in information they voluntarily turn over to third parties, the SCC has rejected such a categorical approach for a more holistic methodology.[120] In the Canadian context, the lack of control over information and the existence of a contractual and statutory relationship with a third party does not in and of itself defeat a reasonable expectation of privacy.[121] Rather, the terms governing the relationship between a commercial entity and its users are to be weighed in the totality of the circumstances underpinning the expectation of privacy analysis.[122] As can be discerned, there is a significant difference between U.S. and Canadian search and seizure law in terms of information held by third parties. This likely separates the legal conclusions that may be reached by the U.S. and Canada in terms of a reasonable expectation of privacy in user information on a cryptocurrency exchange. While US law would deny such an expectation based on the third-party doctrine, this paper contends that Canadian law would recognize such an expectation, albeit in a diminished capacity.

In *Gomboc*, the ability of a commercial entity to disclose users' information was deemed to factor heavily against a finding of a reasonable expectation of privacy.[123] Ignorance of such terms by a claimant is no defence; as recognized in *Spencer*, a reasonable user would be aware of the terms and conditions underpinning a service they are utilizing.[124] In regards to crypto exchanges, the terms and conditions of the largest and most used exchange, Binance, will be utilized as an example for this analysis.[125] Under

---

119 See *Tessling, supra* note 41 at para 32.

120 See *United States v Miller*, 425 US 435 (5th Cir, 1976). See also *Gratkowski*, *supra* note 73 at 4-6.

121 See *Gomboc*, *supra* note 45 at para 28; *Cole*, *supra* note 38 at paras 54, 58; *Marakah*, *supra* note 42 at para 38; *Jones*, *supra* note 42 at paras 40-45; *Spencer*, *supra* note 42 at paras 46, 54.

122 See *Gomboc*, *supra* note 45 at para 31.

123 *Ibid* at para 33.

124 See *Spencer*, *supra* note 42 at para 57.

125 See Coinmarketcap, "Top Cryptocurrency Spot Exchanges" (accessed 18 March 2022), online: *CoinMarketCap* <coinmarketcap.com/rankings/exchanges/> [perma.cc/V24B-J4F7]. It should be noted that after the writing of this paper, Binance has announced

Binance's terms of use, their privacy policy is a supplemental contractual term to those terms of use and a user must agree to them to use the platform.[126] Binance's privacy policy states "we may share your personal data with third parties" including "to legal authorities to the extent we are obliged to do so according to the law. We may also need to share your information to enforce or apply our legal rights or to prevent fraud."[127] The terms of use also indicate that Binance has the right to unilaterally investigate and determine whether you have breached their terms and, without consent or prior notice, report an incident to authorities.[128] This indicates that Binance will disclose a user's personal information to authorities if compelled to do so legally, or voluntarily if they suspect a user is engaged in activities which breach their conditions. In this sense, it cannot be said that there is an obligation of confidentiality attached to a user's information on Binance. A reasonable user of Binance's platform would be aware of these underlying terms and the power they give to Binance to divulge their information. Similar to *Gomboc*, the fact that Binance is free to disclose information to authorities if compelled or if they so choose, militates against finding a reasonable expectation of privacy in user information on crypto exchanges.[129] However, the court in *Gomboc* held that this is not dispositive of the objective reasonableness inquiry, instead stating that the question is "whether the information is the sort that society accepts should remain out of the state's hands because of what it reveals about the person involved."[130] With this in mind, it is prudent to turn to the privacy interests implicated by a search for user information on a cryptocurrency exchange.

Shifting the focus to the privacy interests engaged by state conduct, it must be determined whether the information sought tends to reveal a biographical core of personal information. The court in *Spencer* held that "subscriber information, by tending to link particular kinds of information

---

that it is withdrawing its services from the Canadian marketplace in late 2023 due to tightening regulations. See Craig Lord, "Binance, the world's biggest cryptocurrency exchange, is leaving Canada" (12 May 2023), online: *Global News* <globalnews.ca/news/9694837/binance-leaving-canada-crypto/> [perma.cc/PXR3-9MZ9].

126 See Binance, "Binance Terms of Use" (8 February 2023), online: *Binance* <www.binance.com/en/terms> [perma.cc/76G2-PEQL].

127 Binance, "Privacy Notice – Binance" (29 September 2022), online: *Binance* <www.binance.com/en/privacy> [perma.cc/X29K-3P62].

128 See Binance, "Binance Terms of Use" (8 February 2023) online: *Binance* <www.binance.com/en/terms> [perma.cc/BP34-E4D7].

129 See *Gomboc*, *supra* note 45 at para 33.

130 *Ibid* at para 34.

to identifiable individuals, may implicate privacy interests relating not simply to the person's name or address but to his or her identity as the source, possessor or user of that information."[131] This is analogous to a situation where authorities seek user information from a cryptocurrency exchange. The privacy interests implicated are beyond the name, address, email or phone number of the user. Instead, authorities wish to utilize this information to link an identifiable individual to a specific exchange wallet address. In this sense, the privacy interests engaged relate to the information that can be elicited from the connection of that person to the wallet. United States jurisprudence has taken a narrower view of a search of cryptocurrency exchange records, finding that "it provides only information about a person's virtual currency transactions."[132] However, by utilizing the blockchain to look at that wallet address, authorities can discern a quantum of information far beyond mere transaction data. As illustrated above in examples 1 and 2, the information revealed includes what transactions an individual has made, when they made them, how much money was implicated in those transactions, and what cryptocurrencies that individual has on that wallet address. Similar to the search of cryptocurrency storage mediums, the subject matter of the search for user information on a crypto exchange can reveal an individual's financial holdings and preferences. This uncovers the intimate details and personal lifestyle choices of an individual in numerous ways. It allows the state to know what cryptocurrencies an individual chooses to hold in their exchange wallet, the exact time that the individual transacts, and the overall amount of the transaction. Knowing the exact time that an individual transacts also reveals to the state exactly when that individual was connected to the internet. Considering the purview such a search can provide into one's personal financial preferences, choices, and dealings, the privacy interests engaged arguably militate in favour of a reasonable expectation of privacy.

Balancing the circumstances, it is true that there is a lack of control over user information on cryptocurrency exchanges and that contractual terms, at least concerning the largest cryptocurrency exchange, do not have an obligation of confidentiality vis-à-vis that information. While this militates against a reasonable expectation of privacy, and a lack of third-party confidentiality factored heavily into the decision rendered in *Gomboc*, the court instructed that the central issue in that case still fell upon whether the information at issue disclosed intimate details of an individual's lifestyle

131 *Spencer*, *supra* note 42 at para 47.
132 *Gratkowski*, *supra* note 73 at 8.

and personal choices.[133] The information at issue in *Gomboc*, that being the pattern use of electricity in a home as disclosed by a digital recording ammeter, was held not to divulge any intimate details beyond an individual's consumption of electricity.[134] In contrast, a search of user information on a cryptocurrency exchange can reveal personal financial preferences, choices, and dealings. These privacy interests are far more revealing of one's lifestyle and choices compared to the mere consumption of electricity and allow the state to peer into how one conducts themselves financially. This includes knowing when they transact, for how much, and what cryptocurrencies they choose to hold in their exchange wallet. It is contended that this distinction tips the scale in favour of finding that the expectation of privacy is objectively reasonable as it concerns a search of user information on a cryptocurrency exchange. Similar to *Gomboc*, the lack of control and third-party obligations of confidentiality hinder this expectation. But unlike *Gomboc*, there are privacy interests at stake with the capacity to reveal intimate financial details about an individual. Such a conclusion is consonant with the decision rendered in *Gomboc* and follows the SCC's instruction. Namely, that the central question in informational privacy cases concerns the ability of the impugned search to reveal intimate details about one's lifestyle and choices.[135] It is, however, conceded that the lack of control and confidentiality as it concerns this information likely diminishes a reasonable expectation of privacy. Accordingly, there is a reasonable, albeit diminished, expectation of privacy in user information on a cryptocurrency exchange.

VII. CONCLUSION

This paper set out to address the void in Canadian jurisprudence as it relates to section 8 of the *Charter* and cryptocurrency. How the reasonable expectation of privacy applies to cryptocurrency transaction data on the blockchain, different methods of storing cryptocurrency, and user information on cryptocurrency exchanges was explored. Three contentions were sought to be made concerning this investigation: that there is no reasonable expectation of privacy in cryptocurrency transaction data on the blockchain; that there is a reasonable expectation of privacy in various types of cryptocurrency storage mediums; and that there is a diminished reasonable expectation of privacy in user information on cryptocurrency

133 See *Gomboc*, *supra* note 45 at para 34.
134 See *Gomboc*, *supra* note 45 at paras 1, 14, 39.
135 See *Gomboc*, *supra* note 45 at para 34.

exchanges. Following an explanation of cryptocurrency, the blockchain, and the jurisprudence relating to s. 8 of the *Charter*, these arguments were meticulously examined and substantiated by thorough analysis.

The inherently public nature of the blockchain, paired with the fact that a search of the blockchain does not itself reveal the identity of an individual behind a crypto wallet address, was deemed to thwart any conception that there is a reasonable expectation of privacy in cryptocurrency transaction data on the blockchain. Anyone with access to the internet can browse a blockchain's records as its very purpose is to display this information in the wide open for public view. In further support of this proposition, United States jurisprudence that echoed similar thoughts was cited.[136] On the premise of these considerations, it was determined that there is no reasonable expectation of privacy as it relates to cryptocurrency transaction data on the blockchain.

In terms of mediums of cryptocurrency storage, three types were explored. These were desktop, mobile, and hardware wallets. It was discovered that the search of these types of wallets necessarily occurs on an individual's personal device, which essentially connects that individual to the searched crypto wallet as authorities will almost always know who owns the device being searched. This allows the state to personally identify an individual with the informational content on the searched cryptocurrency storage medium. Such information reveals intimate details about an individual's lifestyle and choices as it exposes to the state how much money an individual holds in crypto, what crypto assets they hold and have previously held, and when and for how much they have made transactions with those assets. By exposing an individual's financial preferences, holdings, and when and how they choose to spend their money, the search of a cryptocurrency storage medium was held to implicate significant informational privacy interests relating to one's lifestyle and personal choices. An individual's control over the informational content of their cryptocurrency storage mediums was also explored. It was determined that individuals undoubtedly exercise meaningful control over these cryptocurrency storage mediums as they are contained on, or are themselves, personal devices in the individual's possession. Considering all these elements, they were found to militate in favour of the notion that there is a reasonable expectation of privacy in desktop, mobile, and hardware cryptocurrency storage wallets.

The reasonable expectation of privacy in user information on cryptocurrency exchanges was analyzed last. However, it was also established that a search of user information on a cryptocurrency exchange

---

136 See *Gratkowski*, *supra* note 73 at 6-7.

can reveal details about an individual's lifestyle and personal choices. The privacy interests implicated in such a search were held to go beyond merely the name, address, email, or phone number of the user. Rather, authorities would utilize this user information to link an identifiable individual to a specific exchange crypto wallet address. Consequently, this allows law enforcement to attach that individual to a specific exchange crypto wallet address and browse its data on the blockchain. This exposes to the state information relating to the exact time that individual transacts, how much they transact for, and what cryptocurrencies an individual chooses to hold in their exchange wallet. Based on the tendency of such information to reveal one's personal financial preferences, choices, and dealings, the privacy interest engaged by a search of user information on a cryptocurrency exchange was held to weigh in favour of a reasonable expectation of privacy. Balancing the privacy interests at stake with the lack of control and confidentiality, and utilizing the SCC's instructions and language from *Gomboc,* it was concluded that there is a reasonable but diminished expectation of privacy in user information on a cryptocurrency exchange.

Ultimately, the perpetual evolution of technology inevitably carries with it the reality that it can, and will, be utilized in some form of criminal enterprise. The law must adjust quickly and pragmatically to ensure law enforcement has a degree of guidance in their attempts to combat contemporary techniques of engaging in criminal activity. In this quest for adaptation, the law must tread carefully and appropriately balance the public's privacy interests with the state's pursuit of crime control. After all, it would be tragic to witness privacy become a sacrificial lamb as the state attempts to adjust to contemporary technologies.

Perhaps a solution to the tension between crypto's use in criminal enterprise and the maintenance of public privacy lies in the regulatory clarity provided by parliament. While the substantive nature of such regulation is beyond the breadth of this paper, regular disclosure of crypto assets by crypto exchanges and financial institutions, paired with reporting to tax authorities on large-scale crypto transactions, could help to combat the risks posed by crypto. Doing so could alleviate the possibility of another exchange like FTX defrauding customers of millions of dollars. This could also potentially prevent other crimes such as money laundering by requiring the reporting of large-scale crypto transactions to tax agencies like the CRA. Considering the 2023 federal budget explicitly dedicates resources to protecting Canadians from the risks of crypto, it is safe to say that these speculated changes may indeed be on the horizon.[137]

---

[137] See Canada, Department of Finance, *Budget 2023,* (Ottawa: Government of Canada, 2023) at 175-176.