CITATION: Durham Regional Police Service (Re), 2024 ONSC 1928
COURT FILE NO. CR-23-16189
DATE: 20240402

ONTARIO

SUPERIOR COURT OF JUSTICE

(Central East Region)

IN THE MATTER OF an order dismissing an application for a general warrant sought by the Durham Regional Police Service pursuant to section 487.01 of the *Criminal Code*;

AND IN THE MATTER OF an order dismissing an application for an assistance order sought by the Durham Regional Police Service pursuant to section 487.02 of the *Criminal Code*;

AND IN THE MATTER OF an application by the Attorney General for Ontario for an order in the nature of *certiorari* with *mandamus* in aid to quash the above-referenced orders and compelling the Provincial Court to exercise its jurisdiction to grant the general warrant and assistance order.

Alysa Holmes and *Michael Fawcett*, for the Attorney General for Ontario
Graeme Hamilton and *Brianne Taylor*, for Binance Holdings Limited
Michael Lacy, *Amicus Curiae*, and with him, *Bryan Badali*

Heard: August 8, 2023

S.T. BALE J.:-

INTRODUCTION

[1] Cybercrime has become increasingly prevalent as commerce moves online. Its proliferation has been accompanied by a corresponding increase in the use of cryptocurrency to facilitate and profit from crime. Because of unique challenges associated with investigating and prosecuting offences using cryptocurrency, foreign criminal actors have increasingly profited from Canadian victims while remaining beyond the reach of our criminal justice system.

[2] In the present case, the victim was tricked into purchasing and transferring Bitcoin worth approximately $65,000 into digital wallets outside his control. Durham Regional Police Service traced a part of the Bitcoin into three digital wallets held on the Binance cryptocurrency exchange. The issue on this application is whether a general warrant may be used to seize cryptocurrency held on a third-party exchange.

[3] In March 2023, DRPS applied for a general warrant and related assistance order under ss. 487.01 and 487.02 of the *Criminal Code*. By means of the warrant and assistance order, police sought to seize the subject cryptocurrency by compelling Binance to transfer it from the suspects' wallets into a secure wallet held by DRPS.

[4] Under s. 487.01 of the *Code*, a judge may issue a warrant authorizing a peace officer to use any device or investigative technique or procedure, or do anything described in the warrant that would, if not authorized, constitute an unreasonable search or seizure if, (a) the judge is satisfied that there are reasonable and probable grounds to believe an offence has been committed and that information concerning the offence will be obtained, (b) the judge is satisfied

that it is in the best interests of justice to issue the warrant, and (c) there is no other provision under the *Criminal Code* or other Act of Parliament permitting the technique, procedure or device or the doing of the thing. Under s. 487.02, the judge or justice who issues the warrant may order a person to provide assistance, if the person's assistance may reasonably be considered to be required to give effect to the warrant.

[5] The DRPS application was dismissed by Burstein J. of the Ontario Court of Justice. In dismissing the application, he found that the application failed to satisfy all three of the preconditions for issuing a general warrant.

[6] The Attorney General for Ontario now applies for orders of *certiorari* and *mandamus* to quash the application judge's order dismissing the DRPS application, and to compel the Ontario Court of Justice to exercise its jurisdiction to issue the requested general warrant and assistance order. The Attorney General argues that general warrants are the only available tool for police to recover cryptocurrency taken from Canadian victims by criminals outside the reach of our criminal justice system, and that in dismissing the warrant application, the application judge committed jurisdictional and legal errors that justify the requested relief.

[7] While also addressing the narrower issue of whether the application judge erred by refusing to issue the proposed general warrant and assistance order, the Attorney General's stated purpose for bringing this application is to confirm, as a matter of law, "the continued availability of general warrants as a method of seizing cryptocurrency from suspect accounts on third-party exchanges – a critical investigative tool in the ongoing fight against cybercrime in this country." Crown counsel argues that this is an issue of national importance.

[8] The suspects in this case are unlikely to face prosecution in Canada. A production order served on Binance confirmed that all three are Nigerian citizens with Nigerian places of residence.

[9] Because it was unlikely that the suspects would take part in the proceedings (and they have not), I appointed *amicus curiae* to assist me in receiving full argument.

[10] For the following reasons, I agree with Burstein J. that the DRPS application failed to satisfy all three of the preconditions for issuing a general warrant. Most importantly, I find that within the meaning of s. 487.01(1)(c) of the *Criminal Code,* there are provisions in the *Code,* other than general warrants, that provide for a warrant, authorization or order permitting police to seize cryptocurrency, and hold it in a secure wallet for return or forfeiture. In particular, I refer to special warrants – digital assets (s. 462.321) and restraint orders (s. 462.33), combined with management orders (s. 462.331).

[11] The application will therefore be dismissed.

AVAILABILITY AND SCOPE OF *CERTIORARI* REVIEW

[12] Before explaining why I find there to be "other provisions" providing for the technique sought to be used by the DRPS, I will deal briefly with the availability and scope of *certiorari* review.

[13] Although unaware of any *certiorari* applications relating to a refusal by a provincial court judge to issue a general warrant, the Attorney General submits that such review should be

available, based upon the availability of *certiorari* review in relation to decisions concerning other *Criminal Code* investigative devices, such as conventional search warrants and production orders. I agree. See *textPlus Inc. (re)* (2022), 163 O.R. (3d) 737, [2022] O.J. No. 4959, at paras. 38–48; *R. v. Brown*, 2015 ABQB 728, at para. 40; *British Columbia (Attorney General) v. Brecknell*, 2018 BCCA 5; and *R. v. Brown*, 2019 ONSC 5032.

[14] However, the question of the available scope of that review is more difficult. In the context of criminal trial proceedings, *certiorari* is only available when the lower court commits jurisdictional error. A court will fall into jurisdictional error if it errs in its interpretation of a statute that is jurisdictional in nature, refuses to exercise its jurisdiction, or acts in breach of principles of natural justice: *R. v. Awashish*, 2018 SCC 45, at paras. 20-24.

[15] The Attorney General argues that the scope of *certiorari* review of a refusal to grant an application for an order relating to a *Criminal Code* investigative tool should be broader, and requests a ruling that *certiorari* may be granted, based on an error of law alone, in the context of a provincial court's dismissal of an application for a warrant or other investigative device. However, given my conclusion that the application judge committed no error in declining to issue the general warrant, it is unnecessary for me to consider this issue.

THE APPLICATION JUDGE'S REASONS

[16] Referring to the "no other provision" precondition in s. 487.01(1)(c) of the *Code*, the application judge found that the general warrant sought by the DRPS was aimed at recovering property obtained by the commission of an offence, and that there were a variety of other "legal mechanisms" that would have authorized them to do that. In particular, he held that a restraint order under s. 462.33 of the *Code* would have allowed the Attorney General to apply for an order prohibiting Binance from "disposing of, or otherwise dealing with, any interest in the property specified in the order." He pointed out that even if it could be said that the cryptocurrency is not "within a province", s. 462.33(3.1) of the *Code* provides that "[a] restraint order may be issued under this section, in respect of property situated outside Canada."

[17] The application judge found that the materials filed by the DRPS in support of the general warrant would likely have satisfied the requirements for obtaining a restraint order under s. 462.33. However, he concluded that even if there is "no other provision" authorizing the technique, the appropriate remedy is for Parliament to address the problem, not the courts.

[18] The application judge noted that the *Criminal Code* allows police "to seek authorization for the seizure of property for a variety of reasons, such as to afford evidence of a crime, to remove dangerous contraband from the public domain and to compensate victims for harms suffered", and said that he was not satisfied that it would be "legally appropriate to seek a general warrant for the purpose of seizing suspected proceeds of crime."

ANALYSIS

Central issue

[19] The central issue in this case is whether there are provisions of the *Criminal Code* or other Act of Parliament, other than a general warrant and assistance order, that would provide for a warrant, authorization or order permitting the technique proposed by the DRPS.

The technique proposed by the DRPS

[20] The first step in the analysis is to identify the proposed "technique, procedure or device to be used or the thing to be done." For convenience, I will consolidate those terms and refer to them as the "technique".

[21] The technique proposed by the DRPS is variously described. For example, in the ITO, DC Snow deposed that "[t]he general warrant will allow the police to seize the subject cryptocurrency and facilitate its forfeiture as proceeds of crime or its return." In argument, Crown counsel described what the police sought to do was to "compel Binance to transfer the subject cryptocurrency into the direct and exclusive control of the police in order to facilitate a final determination of lawful ownership under the court's supervision." The draft order which the application judge was asked to sign provided for the transfer of the subject cryptocurrency to a secure wallet held by the DRPS and required Binance to facilitate the transfer.

The general warrant – s. 487.01 of the *Code*

[22] General warrants are provided for in s. 487.01 of the *Criminal Code*:

> 487.01 (1) A provincial court judge, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 may issue a warrant in writing authorizing a peace officer to, subject to this section, use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person's property if
>
> > (a) the judge is satisfied by information on oath in writing that there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed and that information concerning the offence will be obtained through the use of the technique, procedure or device or the doing of the thing;
> >
> > (b) the judge is satisfied that it is in the best interests of the administration of justice to issue the warrant; and
> >
> > (c) there is no other provision in this or any other Act of Parliament that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done.

[23] This provision was introduced by Parliament in 1993 to fill any potential gaps in the availability of judicial authorizations to conduct searches and seizures. The provision "recognizes that Parliament cannot anticipate or imagine all investigative means or techniques that are or will become available to the police": *R. v. Ha,* 2009 ONCA 340, at para. 26.

[24] The leading case on the availability of general warrants is *R. v. TELUS Communications Co.*, 2013 SCC 16. The question in *Telus* was whether the police were entitled to a general warrant or whether they required a "wiretap authorization" pursuant to Part VI of the *Code.*

[25] Part VI provides for the interception of private communications. Under s. 185, the Attorney General, the Minister of Public Safety or a designated agent may apply for a wiretap authorization. In Ontario, the Crown agent is usually an assistant crown attorney or public prosecutor designated for that purpose.

[26] In *Telus,* the police had obtained a general warrant and related assistance order under ss. 487.01 and 487.02 of the *Criminal Code.* The orders required Telus to provide the police with stored text messages sent or received by two Telus subscribers, on a daily basis. Telus applied to quash the general warrant arguing that the prospective daily acquisition of text messages would require an authorization under Part VI of the *Code.* The application judge dismissed the application. On appeal to the Supreme Court of Canada, it was held that the general warrant was invalid because the investigative technique that it authorized was substantively equivalent to what would have been done pursuant to a Part VI authorization.

[27] The following principles emerge from the reasons in *Telus:*

- section 487.01(1)(c) should be broadly construed to ensure that general warrants are not used presumptively. This is to prevent circumvention of more specific or rigorous preauthorization requirements (at para. 19);
- the focus is on the actual substance of the investigative technique, not merely its formal trappings. The provision must be interpreted to afford the police the flexibility Parliament contemplated in creating the general warrant, while safeguarding against its misuse (at para. 77);
- there is a need for heightened judicial scrutiny where Parliament has provided an authorization for an investigative technique that is substantively equivalent to what the police seek but requires more onerous pre-conditions (at para. 77);
- courts must be careful to fill a legislative lacuna only where Parliament has actually failed to anticipate a particular search authorization. To do otherwise would chip away at the foundation that shapes the respective roles of the courts and Parliament in our system of criminal justice when individual rights and freedoms are at stake (at para. 78); and
- although the provision is broad and can capture almost any kind of investigative technique or procedure, "history confirms that general warrants were to play a modest role affording the police a constitutionally sound path for investigative techniques that Parliament had not addressed" and are properly construed as "rearguard warrants of limited resort, not frontline warrants of general application" (at para. 93).

Other provisions that would provide for a warrant, authorization or order permitting the technique sought to be used by the DRPS in the present case

[28] Under Part XII.2 of the *Criminal Code* – entitled "Proceeds of Crime" - there are other provisions providing for a warrant, authorization or order permitting the technique sought to be used by the DRPS in the present case. Part XII.2 provides for both restraint orders and special warrants – digital assets. Either may be combined with a management order.

Restraint orders

[29] Restraint orders which prohibit "any person from disposing of, or otherwise dealing with any interest in, the property specified in the order" are available on application by the Attorney General where the judge is satisfied that there are reasonable grounds to believe that "there exists … any property in respect of which an order of forfeiture may be made under subsection 462.37(1) or (2.01) or 462.38(2) in respect of a designated offence …." Section 462.33(3.1) provides that restraint orders have extraterritorial jurisdiction, including outside of Canada.

[30] Under s. 462.33(7), before a judge makes a restraint order, the judge "shall require the Attorney General to give such undertakings as the judge considers appropriate with respect to the payment of damages or costs, or both, in relation to (a) the making of an order in respect of property situated within or outside Canada; and (b) the execution of an order in respect of property situated within Canada.

Special warrant – digital assets

[31] The application judge based his decision on the availability of restraint orders to do what the police wanted to do, and the argument on the present application focused on the question of whether restraint orders, coupled with management orders, are substantively equivalent to general warrants for that purpose.

[32] However, in June 2023 (several months after the application judge dismissed the DRPS application), Parliament, presumably with knowledge of the challenges to law enforcement posed by cryptocurrency, amended Part XII.2 of the *Criminal Code* to add s. 462.321, providing for the seizure, management, and disposition of digital assets, specifically including virtual currency. The new section came into force on September 20, 2023, and provides:

> 462.321(1) If, on an application of the Attorney General, a judge is satisfied by information on oath in Form 1, varied to suit the case, that there are reasonable grounds to believe that any digital assets, including virtual currency, may be the subject of an order of forfeiture made under subsection 462.37(1) or (2.01) or 462.38(2) in respect of a designated offence alleged to have been committed within the province in which the judge has jurisdiction, the judge may issue a warrant authorizing a person named in the warrant or a peace officer to
>
> > (a) search for the digital assets by using a *computer program*, as defined in subsection 342.1(2); and
> >
> > (b) seize — including by taking control of the right to access — the digital assets, as well as any other digital assets found during that search that the person or peace officer believes, on reasonable grounds, may be the subject of such an order of forfeiture.

[33] Under s. 462.321(5), a peace officer may, with the consent of the Attorney General, return the seized property to the person lawfully entitled to its possession, if (a) the peace officer is satisfied that there is no dispute as to who is lawfully entitled to possession of the seized property; (b) the peace officer is satisfied that the continued detention of the seized property is not required for the purpose of forfeiture; and (c) the seized property is returned before a report is filed with the court clerk under s. 462.321(4)(c).

[34] Under s. 462.321(7), before a judge issues a digital assets warrant, the judge "shall require the Attorney General to give any undertakings that the judge considers appropriate with respect to the payment of damages or costs, or both, in relation to the issuance and execution of the warrant."

[35] Crown counsel argues that because digital assets warrants were not available at the time of the DRPS application, those warrants could not have been taken into account by the application judge. While this is so, I could not be expected to grant the relief sought by the Attorney General – an order of mandamus requiring the provincial court to issue a general

warrant – when, in the meantime, Parliament has provided for a new form of warrant which specifically deals with digital currency.

[36] In any event, the Attorney General's position is that these digital assets warrants do not provide for the technique that the police wanted to use in this case, particularly in cases where the prospect of a domestic prosecution is unlikely. Crown counsel argues that these new warrants are limited by all the same legal and practical challenges that affect the existing restraint and management provisions. It will therefore be convenient to deal with digital assets warrants and restraint orders together.

Management orders

[37] Under s. 462.331 of the *Code*, on application of the Attorney General or of any other person with the consent of the Attorney General, the judge may, with respect to property seized or restrained,

> (a) appoint a person to take control of and to manage or otherwise deal with all or part of the property in accordance with the directions of the judge; and
>
> (b) require any person having possession of that property to give possession of the property to the person appointed to deal with the property.

The Attorney General's position with respect to digital assets warrants and restraint orders

[38] The Attorney General's position is that digital assets warrants and restraint orders are not substantively equivalent to general warrants for the purposes of seizing cryptocurrency under the control of a third-party exchange. In support of that position, Crown counsel raises a number of objections to the use of Part XII.2 applications for that purpose. She argues:

- that unlike applications for general warrants which may be made by police, applications for digital assets warrants and restraint orders may be made by the Attorney General but not by police;
- that unlike with general warrants, multiple applications are required under Part XII.2; and
- that Part XII.2 applications are unavailable in the circumstances of this case because they are limited to the restraint or seizure of any property in respect of which an order of forfeiture may be made under ss. 462.37(1) or (2.01) or 462.38(2) of the *Code.*

[39] Each of these objections may be answered by the simple observation that Parliament, in providing for the search and seizure of proceeds of crime, specifically including digital currency, has legislated the procedures for doing so, and that general warrants cannot be used to circumvent more specific or rigorous preauthorization requirements provided for by Parliament: *Telus,* at para. 19. However, I will go on to specifically address each of the Attorney General's objections

Requirement that Part XII.2 applications be made by the Attorney General

[40] Unlike applications for general warrants which may be made by the police, applications for digital assets warrants and restraint orders may only be made by the Attorney General. Crown counsel argues that this difference is a substantive difference for the purposes of s. 487.01(1)(c). She concedes that the difference is police oversight by the Attorney General but argues that such

oversight is a key part of what makes Part XII.2 applications substantively different from general warrant applications.

[41] However, as Amicus points out, the precondition in s. 487.01(1)(c) is not that there be no other provision that would authorize a particular technique to be used by a peace officer; but rather, that there be no other provision that would authorize the technique, period. Accordingly, on a plain reading of the subsection, the existence of an otherwise substantively equivalent technique will be fatal to the application, whether it is an application that may be made by a peace officer or not.

[42] Crown counsel refers to the fact that the Attorney General and the police are separate and independent entities, and that in any given case, it would be open to the Attorney General to refuse to apply for a digital assets warrant or restraint and management orders that the police wanted to obtain. She argues that it is not a sufficient equivalent to say that some other separate and independent entity could bring a similar application but may or may not decide to do so. She says that there is no "police-led" alternative to a general warrant, for the purpose of bringing the seized funds under the direct and exclusive control of the police, to be returned to the lawful owner, under the court's supervision. In other words, it is the Attorney General's position that the police should be able to seize cryptocurrency on a third-party exchange, by means of a general warrant, even in situations where the Attorney General would not support such a seizure.

[43] In any event, as a practical matter, during an ongoing investigation, the Attorney General does not act independently from the police. The police, in their investigative capacity, bring to the Crown's attention the proceeds to be restrained and managed, and coordinate the application with the Crown. While Crown counsel, representing the Attorney General, oversees and submits the application, typically a police officer involved in the investigation swears the information to obtain.

[44] If Parliament has provided that certain types of searches or seizures should only be the subject of judicial authorization where the Attorney General is the applicant, then that was a decision Parliament made, just as Parliament decided that only an agent designated by the Minister of Public Safety and Emergency Preparedness, or the Attorney General, can apply for a wiretap authorization under Part VI.

[45] Crown counsel further argues that applications for digital assets warrants and restraint orders are substantively different from general warrant applications, because they require the Attorney General to give an undertaking with respect to costs and damages. However, the requirement of an undertaking reflects a policy decision made by Parliament. Parliament has decided that if things are to be seized as alleged proceeds of crime (specifically including virtual currency), there must be oversight by the Attorney General, and that an undertaking must be given with respect to damages and costs.

[46] These safeguards demonstrate Parliament's intention that a higher degree of protection be available where proceeds of crime are seized, including digital currency. Part XII.2 includes more rigorous safeguards than other warrant provisions in the *Code.* In considering whether seizure of cryptocurrency falls within Part XII.2, we must take this overall objective into account. The technical differences relied on by the Attorney General should not be allowed to defeat Parliament's intended protection of those from whom the state intends to seize property.

[47] The decision in *Telus* illustrates the difficulty with Crown counsel's argument. Where the police want to obtain evidence from a telecommunications server, they may obtain copies of historical communications relying on conventional search warrants or production orders. However, there is no specific statutory mechanism available to peace officers to apply for judicial authorization if they want to intercept communications in real time or prospectively.

[48] The fact that the police who had obtained the general warrant in *Telus* could not apply for a Part VI authorization was not a ground for validating the general warrant. In fact, at paras. 73-76, Moldaver J. refers to the fact that only individuals designated by the Minister of Public Safety and Emergency Preparedness or Attorney General may seek a Part VI authorization as one of several more onerous requirements that the police should not be able to avoid by use of a general warrant.

[49] Crown counsel argues that the Attorney General does not take the position that police can use general warrants to access powers that Parliament has specifically reserved to the Attorney General. She argues that while under Part VI, Parliament has provided that only a wiretap agent can apply for a warrant, in the present case, the police are "seeking to do something that they are, in effect, already able to do." She argues that police can apply under s. 487 for a conventional search warrant to seize alleged proceeds of crime such as a bag of cash (where those proceeds are in a building, receptacle or place), and that it is only the intangible nature of cryptocurrency that takes it outside the scope of a s. 487 warrant. While it is true that police often come upon and seize proceeds of crime while executing conventional search warrants, they do so pursuant to s. 489 of the *Code* which provides that a person executing a warrant may, in addition to the things mentioned in the warrant, seize any thing found that the person reasonably believes has been obtained by the commission of an offence. However, if the purpose of the search of a building, receptacle or place is to seize alleged proceeds of crime for potential forfeiture, an application by the Attorney General for a special warrant under s. 462.32 (1) of Part XII.2 is required.

Requirement of multiple orders

[50] Crown counsel argues that unlike general warrant applications, Part XII.2 applications do not provide for a single judicial order, and that three separate orders are required: seizure or restraint, management, and then the ultimate forfeiture or return of the property. There are two basic problems with this argument.

[51] First, even if additional orders were required under Part XII.2, that would be what Parliament has provided where the police seek to take control of proceeds of crime. The fact that the mechanics of obtaining an order allowing the police to take control of the cryptocurrency may be different or more onerous under Part XII.2 does not allow the police to avoid a procedure they dislike and proceed by way of a general warrant application.

[52] Second, in the present case, police sought a general warrant under s. 487.01 and an assistance order under 487.02 in one application. There is no reason why, on a Part XII.2 application, a restraint order or a digital assets warrant, and a management order, could not similarly be obtained on a single application.

[53] Crown counsel argues that even if a restraint order or a digital assets warrant, and a management order were obtained on a single application, Part XII.2 applications are not

substantively equivalent to general warrants because forfeiture or return cannot take place immediately following execution of the digital assets warrant or restraint order, and management order. She argues that the fact that an application for forfeiture or return would have to be made separately, gives rise to a potential for significant delay in disposing of the seized proceeds.

[54] However, this argument is at odds with another argument made by Crown counsel, namely, the argument that the police wanted to seize the funds "to bring them into the criminal justice system, so that a court may dispose of them to their lawful owner, pursuant to the comprehensive *inter partes* regime set out in sections 489.1 and 490 of the *Code*."

[55] The difficulty with the argument is that under s. 490 of the *Code,* further orders would in fact be required for the forfeiture or return of the cryptocurrency. While it is true that under s. 489.1, a peace officer may, without a further order, return the thing seized to the person lawfully entitled to its possession where the peace officer is satisfied that (i) there is no dispute as to who is lawfully entitled to possession; and (ii) the continued detention of the thing seized is not required for the purposes of any investigation or a preliminary inquiry, trial or other proceeding, a similar disposition is available where the seizure is made by means of a digital assets warrant. Under s. 462.321(5) of the *Code*, a peace officer or a person acting on their behalf may, with the written consent of the Attorney General, cause the seized property to be returned to the person lawfully entitled to its possession, if (a) the peace officer is satisfied that there is no dispute as to who is lawfully entitled to possession; (b) the peace officer is satisfied that the continued detention of the seized property is not required for the purpose of forfeiture; and (c) the seized property is returned before a report is filed with the clerk of the court.

Requirement that property to be seized be property in respect of which an order of forfeiture may be made under subsection 462.37(1) or (2.01) or 462.38(2)

[56] Under ss. 462.321 and 462.33 of the *Code,* one of the preconditions for issuing digital assets warrants and restraint orders is that the issuing judge be satisfied that there are reasonable grounds to believe that the property to be seized or restrained may be the subject of an order of forfeiture under ss. 462.27(1) or (2.01) or 462.38(2) of the *Code.*

[57] The Attorney General's position is that in the circumstances of this case, and typically in cryptocurrency cases involving foreign suspects, the procedures in Part XII.2 are not available, because a forfeiture order may only issue upon the laying of charges or after a finding of guilt in a successful domestic prosecution. Because in cryptocurrency cases suspects are generally beyond the reach of the Canadian judicial system, Crown counsel argues that a restraint order is unavailable as a matter of law, because the Attorney General will be unable to establish grounds for belief that "an order of forfeiture may be made."

[58] In making this argument, Crown counsel appears to interpret ss. 462.321 and 462.33 as requiring reasonable grounds to believe that an order of forfeiture will be made. However, in my view, property "may be the subject of an order of forfeiture" where there are reasonable grounds to believe that the property is proceeds of crime obtained through the commission of a designated offence, and that it is not necessary that there be reasonable grounds to believe that an order of forfeiture will be made. I say this because there are dispositions other than forfeiture that property seized under ss. 462.321 and 462.33 may be made. For example, under s. 462.43(1), on application by the Attorney General or any person having an interest in the property or on the judge's own motion, in the prescribed circumstances, the court may revoke the restraint order,

order the property to be returned to the person from whom it was taken or order that it be returned to another person lawfully entitled to its possession.

[59] In addition, although the Attorney General is correct that forfeiture orders under ss. 462.37(1) and 462.37(2.01) require a finding of guilt, in cases where the suspect cannot be brought to justice in Canada, forfeiture may be available under s. 462.38 without a finding of guilt.

[60] Where an information has been laid in respect of a designated offence, section 462.38(2) provides that upon application of the Attorney General, the judge shall order forfeiture, if the judge is satisfied that (a) the property is, beyond a reasonable doubt, proceeds of crime, (b) the property was obtained through the commission of a designated offence in respect of which proceedings were commenced, and (c) the accused charged with the offence has died or absconded.

[61] For the purposes of s. 462.38, an accused will be deemed to have absconded, if (a) an information has been laid, (b) a warrant for the arrest of the person has been issued, and (c) reasonable attempts to arrest the person have been unsuccessful during six months, or "in the case of a person who is not or never was in Canada, the person cannot be brought within that period to the jurisdiction in which the warrant or summons was issued."

[62] Accordingly, the requirement that the property to be seized or restrained be property "in respect of which an order of forfeiture may be made" does not put digital assets warrants or restraint orders beyond the reach of the Attorney General in cases where foreign suspects cannot be brought into Canada.

[63] With respect to s. 462.38, Crown counsel argues that in cases involving foreign suspects, it is unlikely that an information would be laid. But why is that? Parliament has made specific provisions for the forfeiture of proceeds of crime, including digital currency, in the possession of persons who are not or never were in Canada. Proceeds of crime in the possession of such persons is property in respect of which an order of forfeiture may be made, and in swearing the affidavit in support of the application, the deponent may rely on ss. 462.37(1) and 462.38(2) in the alternative: *Laroche,* 2002 SCC 72, at para. 37.

Conclusion on the "no other provision" precondition

[64] On the facts of this case, when one cuts through form and looks at the substance of the search that the DRPS sought to conduct, I conclude that the application judge properly refused to issue the general warrant, because the investigative technique it would authorize was substantively equivalent to what could be done pursuant to a Part XII.2 authorization. In particular, digital assets warrants are tailor-made for the seizure of cryptocurrency held on a third-party cryptocurrency exchange.

Whether the proposed procedure will furnish "information concerning the offence" (s. 487.01(a)), and whether issuing the general warrant would be in the best interests of the administration of justice (s. 487.01(b))

[65] While my finding that there are other provisions in the *Criminal Code* that would provide for a warrant or order permitting the technique for which the DRPS sought a general warrant is

sufficient for the disposition of this application, I will briefly address the "information concerning the offence" and "best interests of justice" preconditions.

Information concerning the offence

[66] The application judge was not satisfied that there were reasonable grounds to believe that "information concerning the offence" would be obtained through the use of the general warrant technique proposed by the police.

[67] Crown counsel argues that that the transferring of the subject cryptocurrency from the target addresses to a police-controlled wallet would represent a confirmation by Binance that the alleged proceeds of crime were, in fact, controlled by the suspects. I disagree and see no basis upon which to infer that the transfer would tell police anything about the offence itself – how it was committed or who committed it. Rather, the transfer would show nothing more than that there was money in the target accounts, that Binance had complied with its undertaking to freeze the accounts, and that it complied with the general warrant and assistance order.

Best interests of justice

[68] It is only where the "no other provision" question is answered in the negative that the inquiry shifts to whether issuance of the warrant is in the best interests of the administration of justice: *Telus,* at para. 96. To illustrate the point, it could not be in the best interests of the administration of justice to allow police to avoid the rigours of an application for a digital assets warrant or restraint order where those authorizations permit the technique or procedure which the police seek to use.

Enforceability of *Criminal Code* warrants and orders against multijurisdictional entities

[69] Binance's position is that the use of a general warrant is not appropriate where police seek to take control of cryptocurrency located in a wallet held on a third-party public exchange.

[70] In support of its position, Binance makes two general submissions. First, while having no comment relating to the tracing method used by DRPS in the present case, Binance argues that as a general matter, block chain tracing is subject to uncertainty and cannot confidently be relied upon to identify that the correct wallet or account is being targeted. Second, Binance argues that ss 489.1 and 490 of the *Code* do not provide affected account holders with an adequate remedy.

[71] However, the issue of greatest concern to Binance is the question of enforceability of *Criminal Code* warrants and orders against multijurisdictional entities.

[72] Binance argues that the seizure of cryptocurrency on a third-party exchange is, in effect, a seizure order *in rem.* Counsel argues that on any jurisdictional analysis, the subject cryptocurrency in this case is not situated in Canada, because Binance is domiciled in the Cayman Islands, and the Binance account holders are resident in Nigeria. Binance's position is that the correct approach to making a seizure in such circumstances – one that is appropriately respectful of international comity – would be to make a mutual legal assistance request to the state in which the property in question resides.

[73] Prior to the hearing, counsel agreed that the application should be bifurcated with the question of enforceability of a general warrant and assistance order, in the circumstances of this

case, to be argued, if necessary, following determination of the question of whether a general warrant and assistance order should otherwise issue. As I have found that a general warrant is not available to the police in this case, the Attorney General may or may not proceed with an application under Part XII.2 of the *Code.*

[74] The Attorney General has agreed to notify Binance if an application under Part XII.2 is made. If such an application is made and the parties wish to argue the issue of jurisdiction, they may contact the trial coordinator to make the necessary arrangements.

DISPOSITION

[75] For the reasons given, the application is dismissed.

"S.T. Bale J."

CITATION: Binance Holdings Limited (Re),
2024 ONSC 1928
COURT FILE NO. CR-23-16189
DATE: 20240402

IN THE MATTER OF an order dismissing an application for a general warrant sought by the Durham Regional Police Service pursuant to section 487.01 of the *Criminal Code*;

AND IN THE MATTER OF an order dismissing an application for an assistance order sought by the Durham Regional Police Service pursuant to section 487.02 of the *Criminal Code*;

AND IN THE MATTER OF an application by the Attorney General for Ontario for an order in the nature of *certiorari* with *mandamus* in aid to quash the above-referenced orders and compelling the Provincial Court to exercise its jurisdiction to grant the general warrant and assistance order.

REASONS FOR JUDGMENT

S.T. BALE J.

April 2, 2024