
CANADA / JUDGMENT

U.S.A. v. Su Bin

2015 BCSC 1586

COURT

Supreme Court of British Columbia

DECIDED

2 September 2015

Source: bccourts.ca · Research copy typeset by Esheria. Not court-issued or certified.

2015 BCSC 1586 U.S.A. v. Su Bin

IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation:

U.S.A. v. Su Bin,

2015 BCSC 1586

Date: 20150902

Docket: 26595

Registry: Vancouver

In the Matter of the Extradition Act,

S.C. 1999, c. 18, as amended

and

In the Matter of

The Attorney General of Canada

on behalf of the United States of America

and

Su Bin

aka Stephen Su

aka Stephen Subin

Before: The Honourable Mr. Justice Greyell

Oral Reasons for Judgment

Counsel for the Attorney General of Canada on behalf of the Requesting State:

D.J. Strachan

D.B. Majzub

G. Jamieson, A/S

Counsel for the Person Sought:

G. DelBigio, Q.C.

Place and Date of Trial/Hearing:

Vancouver, B.C.

July 8 & 9, 2015

Place and Date of Judgment:

Vancouver, B.C.

September 2, 2015

Introduction and Background

- [1] The United States is seeking the extradition of Su Bin (a.k.a. Stephen Su, a.k.a. Stephen Subin, a.k.a. Steven Subin) ("Su") for prosecution for conspiracy with two unindicted co-conspirators ("Co-con1" and "Co-con2") and others to access business computer networks without authorization and to steal valuable and proprietary technical information, specifically military and aviation information relating to C-17, F-35 and F-22 military aircraft, amongst others.
- [2] The Minister of Justice has issued an Authority to Proceed ("ATP") dated September 19, 2014 under s. 15 of the Extradition Act, S.C. 1999, c.18 [Act]. The ATP authorized the Attorney General of Canada ("Attorney General") to seek an order of committal for the corresponding Canadian offences of unauthorized use of a computer, contrary to s. 342.1 of the Criminal Code, R.S.C., 1985, c. C-46 [Code], and the communication of any sketch, plan, model, document or information relating to a munition of war to a foreign power, or in any other manner prejudicial to the safety or interests of the State., contrary to s. 4(2) of the Security of Information Act, R.S.C., 1985, c. O-5 [SIA].
- [3] The request to extradite Su is supported by a Record of the Case ("ROC") dated August 21, 2014, a First Supplemental Record of the Case dated September 18, 2014 ("FSROC") and a second Supplemental Record of the Case dated March 10, 2015 ("SSROC"). Each of the ROC, FSROC and SSROC has been certified by Assistant United States Attorneys. I will collectively refer to the ROC, FSROC and SSROC as the "ROCs".

- [4] By way of overview, the United States asserts Su, with Co-con1 and Co-con2, who are alleged to be Chinese military officers, accessed confidential proprietary military and aviation technology on the computer servers belonging to aircraft manufacturers Boeing, Lockheed Martin, Exelis and Airbus relating to various military aircraft manufactured by those companies. The unauthorized access is alleged to have occurred between 2009 and 2012.
- [5] The Attorney General submits that a reasonable, properly instructed jury could use the evidence contained in the ROCs to find that Su had committed the offences in s. 342.1 of the Code and s. 4(2) of the SIA and, hence, the evidence is sufficient to commit Su for extradition for prosecution.
- [6] Counsel for Su submits the Attorney General has not proven the person before the court is the person named in the ROC. Alternately, counsel says the information contained in the ROC is vague, lacks specificity and fails to meet the test that a properly instructed jury could find Su committed the specified offences.

Legal Framework for the Extradition Committal Hearing

- [7] Section 3(1) of the Act provides for extradition from Canada on the request of an extradition partner for the purpose of prosecuting the person sought if:
- (a) the offence in respect of which the extradition is requested is punishable by the extradition partner, by imprisoning or otherwise depriving the person of their liberty for a maximum term of two years or more, or by a more severe punishment; and
 - (b) the conduct of the person, had it occurred in Canada, would have constituted an offence that is punishable in Canada,
- (ii) by imprisonment for a maximum term of two years or more, or by a more severe punishment
- [8] The foreign element of this "double criminality" test is assessed by the Minister of Justice prior to issuing an ATP; the domestic element of the test is assessed by a judge at an extradition hearing: *Canada (Justice) v. Fischbacher*, 2009 SCC 46 at para. 35.
- [8] The test for committal by an extradition judge is set out in s. 29(1) of the Act:
29. (1) A judge shall order the committal of the person into custody to await surrender if
- (a) in the case of a person sought for prosecution, there is evidence admissible under this Act of conduct that, had it occurred in Canada, would justify committal for trial in Canada on the offence set out in the authority to proceed and the judge is satisfied that the person is the person sought by the extradition partner;
- [9] The test was recently reiterated by our Court of Appeal in *United States of America v. Doak*, 2015 BCCA 145 at para. 54:

- [54] The purpose of a committal hearing is to determine whether there is a sufficient case put forward by the requesting state to justify committing for trial in a foreign jurisdiction. As the Court in Ferras explains at para. 9, the test for committal for extradition is the same as that employed by a trial judge in deciding whether to withdraw a case from the jury: whether there is any evidence upon which a reasonable jury properly instructed could return a verdict of guilty. Considering the merit of a particular defence is outside the scope of that inquiry.
- [10] The extradition judge is, thus, required to determine the following matters: (1) what evidence is admissible under the Act; (2) whether the person before them is the person sought by the extradition partner; and (3) whether the admissible evidence is sufficient to justify committal.
- [11] If satisfied that the test for committal has been met, an order for committal of the person sought is issued to await surrender. Then the matter is returned to the Minister of Justice who makes the final decision as to whether to surrender the person to the requesting state: *United States of America v. Ferras*, 2006 SCC 33 [Ferras] at para. 7.

Admissible Evidence

- [12] The evidence admissible at an extradition is set out in s. 32 of the Act:
32. (1) Subject to subsection (2), evidence that would otherwise be admissible under Canadian law shall be admitted as evidence at an extradition hearing. The following shall also be admitted as evidence, even if it would not otherwise be admissible under Canadian law:
- (a) the contents of the documents contained in the record of the case certified under subsection 33(3);
 - (b) the contents of the documents that are submitted in conformity with the terms of an extradition agreement; and
 - (c) evidence adduced by the person sought for extradition that is relevant to the tests set out in subsection 29(1) if the judge considers it reliable.
- [13] Section 33(1) provides:
33. (1) The record of the case must include
- (a) in the case of a person sought for the purpose of prosecution, a document summarizing the evidence available to the extradition partner for use in the prosecution;
- [14] As held in Ferras at para. 54, an extradition judge has the discretion to reject evidence shown to be manifestly unreliable or unavailable for trial if it would make it dangerous or unsafe to commit the person sought on the basis of such suspect evidence.

- [15] The ROC and FSROC were certified by Assistant United States Attorneys for the Central District of California, Anthony J. Lewis and Aaron Lewis and the SSROC was certified by Assistant United States Attorney Anthony J. Lewis. In each case the attorneys certify the evidence summarized in the attached document is available for trial and is sufficient under United States law to justify prosecution: s. 33(3)(a). Therefore, it is presumed to meet threshold reliability and availability for the purposes of committal.
- [16] While there is no challenge to the presumed admissibility of the ROCs in this case, counsel for Su challenges the reliability of the evidence contained in the ROCs.
- [17] Counsel for Su argued there was no evidence Su had authored or received any of the e-mails passing between his e-mail address(es) and Co-con 1 and/or Co-con 2; that the evidence relied on by the requesting state that Co-con 1 and Co-con 2 were Chinese military officers and acting on behalf of the Chinese government was not a supportable conclusion based on the content of the e-mails passing between the two; that even if Su had been involved in the exchange of e-mails with either co-conspirator there was insufficient evidence to establish the documents accessed were protected and subject to restricted access, that the requesting state was relying on assumptions drawn from many of the e-mails without providing detail to support the drawing of such assumptions.
- [18] Counsel for Su argued the Attorney General had not established either the actus reus or mens rea had been made out to establish the commission of the offences alleged under s. 342.1 of the Code or s. 4(2) of the SIA.
- [19] Counsel for Su argued a properly instructed jury acting reasonably could not reach a verdict of guilty in Canada: *United States of America v. Graham* (2007), 222 CCC (3rd) 1 at para. 32, *U.S.A. v. Robertson*, 2012 BCSC 1800 at para 14; that an extradition judge is not simply to "rubber stamp" an application but is required to examine the quality of the evidence and disregard that which is unreliable or unavailable before assessing the remaining evidence to determine whether it meets the test for committal.
- [20] Counsel argued if the United States wanted to rely on the evidence concerning metadata the ROC has not established the expertise of Special Agent Almeda ("SA Almeda") of the Federal Bureau of Investigation ("FBI") to give opinion evidence about the nature of the meta data.
- [21] Counsel also argued there is no evidence to establish the e-mails of August 6, 2009 (which I will review below) constituted a direction to Co-con 1 and Co-con 2 as to who or what to target. Su's counsel submits the requesting state has not established sufficient evidence exists "in furtherance of" a conspiracy. Counsel submits even if the court is satisfied the data "was obtained or intercepted" by Co-con 1 and/or Co-con2 in concert for a common purpose and that Co-con1 transmitted the data to SU, the transmission per se was not an act in furtherance the conspiracy of "obtaining or intercepting" the data: that the Canadian offence had nothing to do with use of computer information.

[22] Council for Su argued the United States had failed to establish under s. 342.1 of the Code that Su had acquired or obtained the data fraudulently or without colour of right. Counsel says the "warnings" noted on the documents was not sufficient enough to meet the test to warrant committal. Counsel says the United States case is speculative in drawing a conclusion. Su knew the data was restricted simply because he operated an aviation company.

Identification

[23] In *Danielson v. United States of America*, 2008 BCCA 519, Mr. Justice Chiasson identified the two issues of identification in an extradition hearing at para. 24:

1. on a balance of probabilities is the person before the court the person named in the ROC;
2. is there a prima facie case that the person before the court is the person who engaged in the alleged conduct that underlies the request for extradition?

[24] He went on to say at para. 25:

[25] Expressed in this way, it is seen that in many cases the inquiry under both identification issues will involve the same information although the onus of proof differs. For example: the evidence in the ROC contains a photograph which is used by witnesses to identify the person linked to the alleged illegal conduct and the same photograph is used by the extradition judge to identify the person in the courtroom.

[25] Section 37 of the Act provides examples of evidence that can satisfy the test for both aspects of identification:

37. The following are evidence that the person before the court is the person referred to in the order of arrest, the document that records the conviction or any other document that is presented to support the request:
 - (a) the fact that the name of the person before the court is similar to the name that is in the documents submitted by the extradition partner; and
 - (b) the fact that the physical characteristics of the person before the court are similar to those evidenced in a photograph, fingerprint or other description of the person.

[26] In this case, counsel for Su contends that it has not been established that the person before the court is the person identified in the ROCs and who was subsequently arrested on June 28, 2012, or that it was Su who received or sent the various emails to and from the addresses alleged to be his email addresses.

[27] I turn first to address the issue of identification.

Identification

On a balance of probabilities, is the person before the court the person named in the ROCs?

[28] The ROC provides the following identifying information for Su:

Date of Birth: May 14, 1965

Place of Birth: People's Republic of China

Citizenship: People's Republic of China

Eye color: Brown

Hair color: Black

- [29] It provides the following aliases for Su: Su Bin, Stephen Subin, Stephen Su and Steven Subin.
- [30] Attached to the ROC is a photograph of Su identified by Customs and Border Protection Officer Masanto as the individual who was in possession of various forms of identification listing his name as Su Bin on December 31, 2012.
- [31] The Attorney General called two witnesses on the issue of the identification, R.C.M.P. Corporals Dean Etienne and Nancy Chahil.
- [32] On June 28, 2014, Cpl. Etienne was assigned to execute an arrest warrant on Su. He was provided with a B.C. licence plate # 696-DDH and the location of the vehicle Su was driving. He located the vehicle then followed it for a while before pulling it over. He identified Su as the driver of the vehicle by asking him his name and by his driver's licence. He then turned Su over to Cpl. Chahil of the R.C.M.P.'s National Security Program who had followed Cpl. Etienne in her vehicle.
- [33] Cpl. Chahil arrested Su and he was conveyed to the Richmond R.C.M.P. headquarters by Cpl. Etienne where he was booked in.
- [34] Cpl. Etienne testified the physical description of the person he arrested was Asian, middle aged, about his height, 30 - 40 lbs heavier than him and he did not recall his hair colour. When asked in direct examination, he testified he "believed" the person in the prisoner's box, dressed "in red", was the person he arrested.
- [35] In cross-examination, he agreed with counsel that the physical description he had given was a generic one that could fit any number of people. He also agreed that the "most he could say" was that the person in the prisoner's box was "maybe" Su.
- [36] Cpl. Chahil had a lengthier involvement with Su on the date of his arrest than did Cpl. Etienne. She asked the driver if he was Su and received an affirmative response. She arrested him and read him his Charter rights, including naming the offences he was being arrested for, advised him of his right to counsel and his right to contact the Chinese consulate. At the detachment she took steps to allow Su to contact a lawyer, made a copy of his driver's licence and generally oversaw the process of his booking in, including being present when his photographs were taken. She also went through his personal effects and wallet, which had been seized when he was arrested. Cpl. Chahil testified she spent between five and five and half hours with Su on the day of his arrest. She identified the person in the prisoner's box was Su, the person who was arrested on June 28, 2014.

- [37] In cross-examination, she agreed that when she came into court to testify she believed she would see the person she arrested in the prisoner's box. Counsel suggested to her she "could not be sure" the person she identified in the prisoner's box was the same person she arrested June 28, 2014. Cpl. Chahil disagreed, testifying she was "sure" the person was Su, the same person she had arrested that day.
- [38] I am satisfied on a balance of probabilities that the person before me is the person arrested on June 28, 2014. The person arrested gave the name Su Bin and produced a driver's licence in that name. Cpl. Chahil had no doubt the person in the prisoner's dock at the extradition hearing was the same person she arrested June 28, 2015. Further, I note a distinct similarity between the person in the photographs depicted on Su's driver's licence, on two of the cards found in his wallet when he was arrested by Cpl Chahil with the person in court in the prisoner's dock and find that person is, indeed, the person arrested on June 28, 2012.
- [39] Furthermore, I am satisfied that the person in court, who was the person arrested on June 28, 2012, is the person named in the ROCs. A comparison of the person before the court with the photograph contained the ROC, establishes this link.

Is there a prima facie case that the person before the Court is the person who sent or received the emails set out in the ROCs upon which the United States relies?

- [40] Su argues there is no evidence he was personally involved in the sending or receiving of the emails sent to email addresses attributed to Su.
- [41] According to the ROC, Su was the head of Lode Technology Co. Ltd. ("Lode Tech"), an aviation technology company with offices in the People's Republic of China ("China"). The United States has preserved a copy of Lode Tech's website which describes Lode Tech as a professional cable harness equipment company that does business in aviation, high speed railway and space sectors and has many global corporate partners. The website describes its business as covering inertial navigation systems, development and integration of aviation airborne software and ground testing software, aircraft power transfer systems, cables and accessories, aeroengine processing equipment and laser technologies. The website also states Lode Tech's engineers have years of experience working for international cable processing corporations and that its engineers include an expert in military cable technology.
- [42] The ROC alleges Su sent and received emails from various email accounts and that he received various emails from Co-con1 and Co-con2 in furtherance of the alleged conspiracies.
- [43] Officer Masanto will testify he was working on December 31, 2012 when Su entered the United States from Canada using a Chinese passport issued February 9, 2009, valid to February 8, 2019. As mentioned, the ROC attaches a photograph of Su taken when he entered Canada on December 31, 2012, which Officer Masanto will confirm is a photograph of the person he inspected.

- [44] He will testify Su filled in a Customs and Border Protection Form I-94 on December 31, 2012 on which he listed an email address "stephensubin@gmail.com". The subscriber records for that particular email account list the subscriber name as "Steve Su" and the SMS phone number as 00 186 139 1102 9729 ("9729"). The Form I-94 listed Su's name as Su Bin and his country of citizenship as "P.R. China". Su produced a Permanent Resident Card from Canada and had in his possession two printed emails, showing they were sent to "subin@lode-tech.com".
- [45] Officer Masanto will also testify he seized two business cards from Su on the same date. One was in the name of "Stevin Subin", listing him as Project Manager for a flight test academy in Africa, with an email address of "subin@lode-tech.com" and the second was a Lode-Tech business card in the name of "Steven Su" with the same email address. The ROC asserts emails sent from this email address contain the last 10 digits of the 9729 number in the signature block and metadata associated with four documents attached to emails sent from this account between January 2010 and May 2012 show the names of "Stephen Subin", "Subin" or "Stephen Su" as the author of or the last person to modify the document.
- [46] Su is also alleged to have used the email addresses "subinstsu@hotmail.com" and "mac.subin@gmail.com". It is alleged the first of these addresses showed the Lode-Tech email address in the signature block as an alternate address and that subscriber records show "Su Bin" as the subscriber's name. The second account lists "Stephen Subin" as the subscriber. The ROC alleges that in July 2009 Su received a draft contract from Co-Con1 addressed to the above Hotmail account which he then forwarded to "mac.subin@gmail.com" and the Lode-Tech email accounts.
- [47] In my view, the evidence establishes there is a prima facie case that the person before the court is the person who engaged in the alleged conduct that underlies the request for extradition. In my view a reasonable jury, properly instructed could conclude from this evidence that Su was the person who sent and received the emails and the attachments to those emails which were sent to or from the email addresses described above.

Sufficiency of the Evidence for Committal

- [48] In *United States of America v. da Silva* (May 3, 2012) Vancouver 25727 (B.C.S.C.), Justice Brown helpfully summarized the principles to be applied by an extradition judge in assessing the sufficiency of the evidence contained in the ROC at para. 16:
- [16] I accept the submissions of the Attorney General that the following principles may be distilled from *Ferras*:
- (a) The inquiry into the sufficiency of the evidence to commit for extradition under s-s. 29(1) involves an evaluation of whether the conduct described by the admissible evidence would justify committal for trial in Canada; whether the evidence exists upon which a reasonable jury properly instructed could return a verdict of guilty.

- (b) The extradition judge's inquiry is focused on conduct; whether the acts disclosed in the admissible evidence are criminal in Canada.
- (c) The extradition judge looks at the whole of the evidence and determines whether it discloses a case on which a jury could convict.
- (d) Evidence that would justify committal in Canada requires at least some evidence on every element of the parallel Canadian crime, the double criminality requirement; however, it is not enough for evidence to merely exist on each element of the crime, the evidence must also be demonstrably able to be used by a reasonable, properly instructed jury to return a verdict of guilty. If the evidence is incapable of demonstrating this sufficiency for committal, then it cannot justify committal.
- (e) The extradition judge does not determine the guilt or innocence of the person sought. That assessment remains for the trial court in the foreign state. However, in order to justify committal, the evidence must establish a case that could go to trial in Canada. This may require the extradition judge to engage in the limited weighing of the evidence to determine not ultimate guilt, but the sufficiency of evidence for committal to trial.
- (f) The extradition judge can refuse to extradite on insufficient evidence such as where the evidence is unavailable or manifestly unreliable. Manifestly unreliable evidence is evidence upon which it would be dangerous or unsafe to rest a verdict.
- (g) In assessing the reliability of the evidence, the extradition judge does not make an actual determination that the evidence is, in fact, reliable. The issue is threshold reliability, whether the evidence tendered possesses sufficient indicia of reliability to make it worth consideration by the extradition judge. The ultimate assessment of reliability is still left for the trial where guilt and innocence are at issue.
- (h) Certification of evidence by the requesting state vests the evidence with a presumption of threshold reliability. Unless rebutted, this presumption will stand.
- (i) Similarly, certification of evidence as available for trial by a requesting state results in a presumption of availability for trial.
- (j) That evidence takes the form of hearsay or is unsworn does not detract from the presumption of threshold reliability.

[49] In *United States of America v. Graham*, 2007 BCCA 345 at para. 32, the court confirmed:

[32] In summary, Ferras stands for the proposition that extradition judges now have the discretion to disregard evidence shown to be unreliable or unavailable and in respect of the evidence that remains, to determine by an assessment of the evidence, including a limited weighing of the evidence, whether it is sufficient for a properly instructed jury acting reasonably to reach a verdict of guilty in Canada.

- [50] The process of limited weighing of the evidence includes an ability to assess the circumstantial evidence to ensure that inferences the requesting state seeks to draw from that evidence are reasonably supportable: *United States of America v. Rosenau*, 2010 BCCA 461 at para. 53; *United States of America v. Dhanda*, 2010 BCCA 200 at para. 37; *R. v. Arcuri*, 2001 SCC 54 at paras. 23, 29 - 30.

Review of the ROCs

- [51] The ROCs contain summaries of the content of emails and information attached to emails to and from the email addresses which are alleged to have been used by Su. The ROCs also summarize the content of emails between Co-con1 and Co-con2 which were not sent to Su. I will not review all of the emails but will focus on a number specifically relied on by the Attorney General.
- [52] The FSROC asserts Co-con1 and Co-con2 are Chinese military officers. It refers to several emails sent between March 2012 and October 2012 purporting to show photographs of Co-con1 and Co-con2 in Chinese military uniforms. In one photograph, attached to an email Co-con1 sent to himself with a header "Boss", Co-con2 was photographed with an unidentified individual. The FSROC further asserts that in an email which I will refer to later as the "C-17 Report" sent by Co-con1 to Co-con2 the former noted, "we [made] important contributions to our national defence scientific research development".
- [53] The ROC alleges that on October 23, 2008, Co-con1 sent an email to another individual seeking to purchase a program called "Poisonivy", a malware designed to capture passwords and transfer files which cannot be detected by anti-virus software.
- [54] SA Almeda, the case agent who is certified as a digital evidence extraction technician and formally trained in conducting computer intrusion investigations, will testify, based on his training and experience, that on August 6, 2009, Su sent Co-con1 an attachment which was an excel spreadsheet listing the email addresses, telephone contact information and program roles for 80 engineers and program personnel working on a specific military project. At the bottom of the email was Su's signature block that listed his mobile telephone number as the 9729 number (discussed above in paras. 38 and 39). SA Almeda will testify he used a portion of the 9729 number as a password and, doing so, was able to open the attachment. He will testify the metadata (which captures the user who last used or edited the document and when that event occurred) on the attached document indicated it was originally created by one of the American companies named in the document. The ROC alleges the specific military project mentioned in the email was one of 32 projects referred to in a subsequent email entitled "complete listing" sent two and one-half years later on February 26, 2012 from Co-con1 to Co-con2. That email listed 32 military projects in one column, a number followed by "M" or "G" and a description of military technology. The ROC alleges that one of the entries on that email related to "F-22" followed by "220M". The United States says this is a reference to the F-22 Raptor military jet which will be described below. SA Almeda is expected to testify "M" and "G" refer to megabytes or gigabytes respectively and

that the total amount of data for all 32 military projects listed on the spreadsheet was 243,585 gigabytes of information. I am satisfied the ROC sufficiently sets out d SA Almeda's qualifications to give this opinion evidence.

- [55] The ROC alleges that on October 1, 2009, Su sent an email to an individual attaching a .rar file describing a specific military technology, containing English and Chinese text and diagrams. A .rar file is a specific format of an archived file that can contain one or more other files in a compressed format. SA Almeda will testify the .rar file was opened using Su's 9729 number as a password.
- [56] The ROC further alleges that on December 14, 2009, Su sent an email to Co-con1 and on December 17, 2009 sent an email to Co-con1 copied to Co-con2. Both emails read "Target" on the subject line and identified certain names, positions, websites, email accounts and companies.

Evidence Related to the Acquisition of Data Regarding the C-17

- [57] Witnesses from Boeing will testify the C-17 "Globemaster" is a military transport aircraft manufactured by Boeing in California and the costs associated with its development and modernization (excluding production related costs) have been approximately 8.9 billion USD. Representatives of Boeing will testify Su did not have authorization to access or possess Boeing data and that such data is not publically available. The data is protected by restricting electronic access, by enforcing contractual provisions on employees and by restricting physical access to Boeing's facilities.
- [58] The ROC asserts that on January 21, 2010, Co-con1 sent Su an email, whose subject line read "C-17 _2", with a file named "C-17 _2.rar" attached. An FBI linguist is expected to testify that in the body of the email, Co-con1 wrote in Chinese: "The password remains unchanged. Please write me a document about which ones are important, which ones are not important and what they are." The ROC states that several further emails passed between Su and Co-con1 which referred to the C-17. On January 26, 2010, Su sent an email to Co-con 1 with the subject line "Re: C-17_2" and attached a 1,467 page word document with a Chinese file name translated as "Appendix-3.docx" ("Appendix 3"). An FBI linguist is expected to testify that in the body of that email Su wrote: "There are many picture documents. The useful ones are marked in yellow. Many documents are for application. They should be the computer documents of a person who uses airplane, not the computer documents of a designer."
- [59] SA Almeda will testify Appendix 3 lists approximately 50,000 files and approximately 142 of the files or folders were highlighted in yellow. He will testify he has reviewed Appendix 3's metadata and it shows "Stephen Subin" as the document's author and the last person to modify it.
- [60] SA Almeda will testify that within the C-17_2.rar file mentioned above, there was a single file folder named "gaga" which contained five document files, four of which contained what he recognized as a directory file listing. A representative of Boeing's Computer Incident

Response Team ("CIRT") will testify that one of the files in the folder named "gaga" listed data files and the names of file folders that were stored on a computer server in Seal Beach, California in 2010 and that one of the other five documents, a pdf, was the same document as one located in Seal Beach titled "Supplemental Flight Manual Mission Computer" which is export-controlled and contains a warning that "[t]his document contains technical data whose export is restricted by the Arms Export Control Act".

- [61] Mr. Follin, a Technical Examiner in Information Security Computer Forensics at Boeing, will testify he examined the contents of Appendix 3 and that many of the files and folder names listed in it match files and folders stored on a Boeing's server located at McChord Air Force Base where Boeing services and maintains the C-17s. SA Almeda compared the list of files on Appendix 3 with the list of files from the forensic copy on Boeing's server and will testify 78% (or 38,866 files) were identical.
- [62] E-mail records show that on March 19, 2010, Co-con1 sent Su an email with a subject translated "View picture" and "Haha" in the body of the email with an image attached entitled "C-17.jpg" which listed seven file names composed of English characters followed by Chinese characters describing their contents. The ROC alleges six of the seven files contained the words "c17" or "c-17" in the name of the file. The files listed are: "Key alloy and metal parts list manual.pdf"; "Task system manual.pdf"; "Generator manual.pdf"; "Hydraulic system manual.pdf"; "Inertia gas system manual.pdf"; "Cockpit glass manual.pdf"; and "Fuel test computer.pdf".
- [63] An FBI linguist will testify Su replied to Co-con1 the same day the March 19, 2010 email was sent with an email containing the words, "Got it".
- [64] Mr. Follin is expected to testify the above file names were stored on Boeing computers. Other Boeing employees will testify they have never seen C-17 files stored on Boeing's computers using Chinese characters as filenames and, in their view, the files listed above were copied, renamed with Chinese characters and saved on a computer outside Boeing's network.
- [65] The ROC asserts email records show that on August 13, 2012, Co-con1 sent Co-con2 an email with the subject line "c17". The email attached a file named in Chinese "C-17 work summary.doc". An FBI linguist will testify the word processing document attached to the email was a report entitled "C-17 Project Reconnaissance Summary Report" ("C-17 Report"). The linguist will testify the C-17 Report contained information from and to other unidentified sources and stated, "we obtained files amounting to 65G" (gigabites of C-17 data) from Boeing's computer network including 630,000 files and 85,000 folders of C-17 data and detailed when and how they carried out the intrusion. Su's counsel argued there was no link between this email and Su.

Evidence Relating to the Acquisition of Data Regarding the F-35

- [66] The F-35 is a fifth generation fighter aircraft with supersonic capabilities equipped with "stealth" technologies that allow it to evade radar. Mr. Korstian, an employee of Lockheed Martin Aeronautical Company ("Lockhead Martin") who is currently an Aeronautical Engineer Principal, will testify the F-35 was developed over many years with multiple companies under contract with the United States Department of Defence at a cost of billions of dollars.
- [67] The ROC asserts email records show that on May 3, 2012, Su sent an email to Co-con1 that contained a subject line which, when translated, read "Plan". Attached to the email was a document related to a flight test plan for the F-35 with different portions written in English and Chinese (the "Flight Test Plan"). The Flight Test Plan had a header in English indicating it was proprietary information belonging to Lockheed Martin and other defence contractors and was subject to export controls. SA Almeda will testify he reviewed the metadata for the document and it identified the author of the document as Mr. Korstian and showed "Subin" as the last person to modify it on March 23, 2012.
- [68] Mr. Korstian will testify he authored the Flight Test Plan for the F-35 and that a comparison between the English language portions of the document attached to the email and the plan he authored showed the English language content of the two was "essentially the same". He will testify there were differences in two of the attached documents where images had been inserted which did not exist at the time the plan was developed.
- [69] Email records show that on February 21, 2013, Co-con1 sent an email to Co-con2 attaching a report which stated "they had acquired data related to both the C-17 and F-35."
- [70] A witness from Lockheed Martin will testify flight test information about the F-35 is not publically available, the aircraft's technical data is protected by restricting electronic access and Lockheed Martin enforces confidentiality clauses in employment contracts.
- [71] Lockheed Martin employees will also testify as to the number of hours, personnel and cost (estimated to be between \$12 - \$15 million) involved in the development of the Flight Test Plan.

Evidence Relating to the Acquisition of Data Regarding the F-22 Raptor Fighter Jet

- [72] The F-22 "Raptor" is a fifth generation fighter jet aircraft that is supersonic, has "super cruise" capabilities and is equipped with "stealth" equipment. The F-22 was developed over multiple years by defence contractors in the United States at a cost of billions of dollars. The particular systems on the F-22 which are relevant to these proceedings are the AVEL (vertical eject launcher) and the AMRAAM (advanced medium range air-to-air missile) systems.

- [73] The ROC alleges that email records disclose that on April 4, 2010, Co-con1 and Su sent each other a total of eight emails with references to "22" in the subject line and attachments to the emails. The first email was from Co-con1 to Su attaching a file titled "22.rar.", which was password protected. The ROC alleges Su responded by email, writing in Chinese, "It's still the information related to the mount." Su then wrote another email to Co-con1 that included the following text: "avel\Training\AVEL Familiarization Course 7-28-08 .ppt". An FBI linguist will testify that in the email Su wrote that Co-con1 should read the document.
- [74] The ROC alleges evidence will establish that Co-con1 then sent five emails in the same email thread to Su, each of which attached a photo of a computer monitor displaying a slide of a presentation about the F-22 AVEL with a proprietary label and export control warning.
- [75] Mr. DeSimini, an engineering fellow at Exelis, the manufacturer of the F-22, who had worked on the AVEL system, will testify he prepared the AVEL slide presentation with others for training purposes in March 2004 with Lockheed Martin and U.S. Air Force personnel. He is expected to testify the five pages from the email records are five pages from the AVEL presentation he prepared.
- [76] Mr. DeSimini will testify the content of the AVEL presentation attached labels indicating it was "EDO [the original developer of the F-22] Proprietary Information", "Source Selection Sensitive" and "This Data is Covered by IATR 22 CFR 120-130" or similar phrasings of these words. The ROC states that IATR should have read ITAR, shorthand for the International Traffic in Arms Regulations. A representative of Exelis will testify information about the F-22 is not publically available; that it was protected by means of restricting electronic access to such information, by restricting physical access to its facilities and by having in place confidentiality agreements with its employees.

Evidence Relating to the Acquisition of Data Regarding the Airbus A400M Military Transport Aircraft ("A400M")

- [77] The ROC asserts email records show that on August 27, 2010, Su sent Co-con1 an email with the subject line "400" and attached a file entitled "400.rar" which was password protected. The ROC asserts that on October 24, 2010, Su sent Co-con1 an email and attached a file entitled "400.rar" which was not password protected and which compressed five word processing documents. The five documents, which are expected to be introduced into evidence at the trial, listed files that refer to the A400M, as well as other Airbus civilian aircraft. Two of the documents which were attached listed a number of files and folders that were highlighted in yellow, including files and folders that contained "A400M" in the document title.
- [78] Mr. Cuadra, former Head of IT Security of Airbus Defence and Space in Spain (where technical data is stored for the A400M), is expected to testify the contents of at least three of the five documents correspond to data that was stored on Airbus's servers in Barajas, Spain in 2010. Mr. Cuadra will testify many of the files corresponding to the filenames relating to the A400M contain business proprietary information about the A400M and some of that

information is subject to export controls in Spain and the European Union. He will further testify that the files are stored on servers in Spain and are not publicly available and that Su was not authorized to access the servers or possess the documents stored there.

Other Data in Su's Possession Relating to the Alleged Conspiracy

- [79] The ROC asserts on November 2, 2011 and twice on November 10, 2011 Su emailed Co-con1 and Co-con2 different versions of a report describing information relating to a specific military project ("Project A"). The metadata for the report showed Su had authored and modified the document. The report Su sent described military data that had been acquired by an entity based in China, claimed to have acquired research and development information that related to Project A that was subject to export restrictions and was restricted by the U.S. Department of Defence, explained why the information was valuable and sought support to complete its work in acquiring more information. The reports were written in Chinese and among the Chinese characters were images embedded that contained diagrams and English language text relating to Project A.
- [80] Email records also show that on October 1, 2009, Su sent an email to another person attaching a .rar file which was opened using Su's mobile telephone number as a password. The file contained a report written in Chinese describing specific military technology and was embedded with diagrams and English language text related to the military technology described in the report.
- [81] SA Almeda is able to testify based on his training and expertise as to certain techniques that are common in the execution of computer intrusions that originate in China that were present in the execution of the scheme allegedly employed between Su, Co-con1 and Co-con2. He will testify that unauthorized access to a computer network can be gained initially through a number of techniques, including by sending emails disguised as legitimate business emails which infect the victim's computer with a virus once an attachment or link is opened. In this case, Su sent emails to Co-con1 and Co-con 2 with the subject line "Target" which identified certain names, email accounts and companies. A report sent from Co-con1 to Co-con2 in an email dated December 27, 2010 described how, because U.S. military science and technology is strictly prohibited, they used techniques like a "business exchange" or "forum salons" to "gain key personnel's relevant information" before laying the path for future "reconnaissance and penetration work".
- [82] SA Almeda will testify about how malicious software, such as the Poisonivy program Co-con1 sought in an email in 2008, works and how, once unauthorized access has been gained, a connection can be established between the victim computer and other computers. He will testify that data gained by unauthorized access is not typically sent directly from the victim's computer to the computer of the one who has accessed it but, instead, "skip routes" or "jump servers" are used to conceal the trail used to send the data. Some of the emails, such as the C-17 Report and the report sent on February 21, 2013 describe how "skip routes" or "jump servers" were used in regards to the acquisition of C-17 and F-35 data.

[83] Finally, SA Almeda will testify that before removing data from a victim's computer, the date is compressed or the file extensions are changed to avoid detection by intrusion detection systems used by the victim's computer. In this case, Co-con1 sent Co-con2 an email describing how they "had to rely on technology to separate and bundle data [and] change the document formats" and that they "avoided the many internal automatic and manual auditing facilities to transfer data safely and smoothly out of the Boeing Company".

U.S. military capabilities and interfering with the design, development or production of weapons and defence equipment intended for U.S. forces. Reliability

[84] Colonel Stephen Russell of the U.S. Air Force will testify the C-17, F-35 and F-22 were developed and produced pursuant to U. S. Department of Defence contracts with aviation and technology companies and that the data related to the C-17, F-35 and F-22 as summarized in the ROC included sketches, plans, models, articles, notes, documents or information that relate to munitions of war and specifically to U. S. military technologies including military aircraft utilized by the U.S. Department of Defence and U. S. Forces. Col. Russell will also testify the communication of this data by Su to a foreign state through Co-con1 and Co-con2 who were Chinese military officers located in China or to third parties for intended sale, is prejudicial to U. S. safety and interests. Counsel for Su submits the evidence contained in the ROCs lacks sufficient detail, is vague, contains unattributed sources of knowledge of fact and is based on speculation and assumptions which are unsupported by the facts and, hence, the evidence is unreliable and forms an insufficient basis for committal.

[85] In particular, counsel for Su argues the United States' case is based on speculation and assumptions drawn, particularly, from the emails between Co-con1 and Co-con2 to which Su was not a party.

[86] Section 33(1) provides the ROC must contain a summary of the evidence available for the purpose of the prosecution of the offences. While I agree Su was not a party to a number of the emails passing between Co-con1 and Co-con2, it would, in my view be open to a reasonable jury, properly instructed, to conclude those emails were in furtherance of emails passing to and from Su and Co-con1 and/or Co-con2. It would be open to such a jury to conclude many of the emails between Co-con1 and Co-con2 contained subject matters discussed in emails between Su and the alleged co-conspirators and were in furtherance of or related to the alleged conspiracy: R. Vu, 2015 BCSC 1073 at paras. 284 and 327; R. v. Yanover (1985), 20 C.C.C. (3d) 300 (Ont. C.A.) at para. 79 .

[87] The evidence set out in the ROCs must be viewed as a whole and in context, not on a piecemeal basis.

[88] Further, as stated recently by Mr. Justice Ehrcke in *United States of America v. Martin*, 2014 BCSC 1112 at para. 41:

Section 33 of the Extradition Act provides that the record of the case should include "a document summarizing the evidence available to the extradition partner for use in the prosecution." It is not required that the record of the case contain a complete and comprehensive statement of all the evidence. In particular, there is no requirement that the ROC describe how each witness knows the things to which he or she will testify.

[89] See also *United States of America v. Doak*, 2015 BCCA 145 at paras. 43 - 46

[90] In my view, the evidence presented by the United States in the ROCs satisfies the test of being sufficiently reliable.

The Canadian Offences

[91] Section 342.1 of the Code provides:

Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction who, fraudulently and without colour of right,

- (a) obtains, directly or indirectly, any computer service;
- (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;
- (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system; or
- (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c).

[92] Section 4(2) of the SIA provides:

Every person is guilty of an offence under this Act who, having in his possession or control any sketch, plan, model, article, note, document or information that relates to munitions of war, communicates it, directly or indirectly, to any foreign power, or in any other manner prejudicial to the safety or interests of the State.

The Criminal Code Offences

[93] Section 342.1(1)(a) provides that it is an offence to fraudulently and without colour of right, directly or indirectly obtain a computer service. "Computer service" is defined in s. 341.1(2) as including data processing and the storage or retrieval of computer data. "Data" is defined as "information or concepts prepared in a form suitable for use in a computer".

[94] In *R c. Parent*, 2012 QCCA 1653 at para. 37, Mr. Justice Gagnon for the Quebec Court of Appeal described the actus reus necessary to prove the offence under s. 342.1(1)(a):

- [37] In this case, in order to prove the actus reus of the offence referred to in paragraph 342.1(1) (a), the appellant had to prove that the respondent had obtained a computer service, that said use was prohibited and that a reasonable person in the same circumstances would have agreed that it was a dishonest activity. The Crown also had to establish that the misappropriation was effected "without colour of right." These elements make up the actus reus of the alleged offences.
- [95] Whether an act is done dishonestly is to be determined objectively by reference to what a reasonable person, placed in Su's circumstances, would consider dishonest: Parent at 34. In *R. c. St-Martin*, 2012 QCCQ 575 at para. 73, the court held that a person fraudulently obtains computer service when he or she, "consciously, intentionally, without error or accident, obtains the service, knowing that he or she does not have the right to do so".
- [96] I agree with the Attorney General that the ROCs provide sufficient evidence whereby a reasonably instructed jury could find that Su, without colour of right, has used or obtained a computer service, the use of which was prohibited, to access and share confidential proprietary information about U.S. and other military aircraft with Co-con1 and Co-con 2 and that a reasonable person in the same circumstances would have agreed that it was dishonest activity.
- [97] It would be open to a jury, properly instructed, to conclude the documents which Su is alleged to have accessed were classified, and that they contained confidential proprietary information not available to the public which Su had no right to access.
- [98] Examples of such obtaining include the sharing of Appendix 3, the Flight Test Plan, the AVEL presentation and the A400M documents.
- [99] Further, there is cogent evidence from which a properly instructed jury could conclude Su took an active role in giving instructions to Co-con1 as to which Boeing C-17 files were "important" and "useful" (in the January 26, 2010 email from Su to Co-con1), highlighting approximately 142 of the 50,000 files. Further, in 2009, Su provided Co-con1 and Co-con2 with information relating to the engineers and program personnel working on a military project. One such email contained the word "Target" in the subject line.
- [100] The requesting state argues that even if the evidence is insufficient to establish Su acted as a principal in fraudulently obtaining a computer service, the evidence is sufficient for a properly instructed jury to conclude Su aided his co-conspirators by purposefully facilitating the commission of the offence under s. 342.1 and, thereby, became a party to the offence pursuant to s. 21(1)(b) of the Code: *R. v. Briscoe*, 2010 SCC 13 at para. 14. I agree that it would be open to a reasonable properly instructed jury to find Su was a party to the commission of an offence under s. 342.1 of the Code.
- [101] Furthermore, I agree there is sufficient evidence for a jury to conclude that the mens rea element of the offence is met; that Su knowingly and deliberately engaged in the impugned conduct. As previously mentioned, many of the documents contained warnings clearly

indicating the files were restricted proprietary information subject to export controls. Su's Project A report to his co-conspirators explicitly acknowledged that fact. There is evidence Su modified documents and actively identified the useful and important files which should be targeted.

- [102] Section 342.1(1)(b) makes it an offence to intercept, directly or indirectly, by means of a device, any function of a computer system. The Code defines "intercept" as including the act of acquiring the substance of a computer system. "Function" is defined as including the storage within a computer system and "computer system" is defined as including a device or group of interrelated devices that contain data. Section 342.1(1)(c) makes it an offence to use, directly or indirectly, a computer system with the intent of committing an offence under s. 342.1 (b). The evidence as set out above in the ROC supports Su's committal for fraudulently intercepting a function of a computer system under s. 342.1(b) and fraudulently using a computer system with the intent to commit that offence under s. 342.1(c).

The SIA Offence

- [103] Section 4(2) of the SIA makes it an offence to possess or control a sketch, plan, model, article, note, document or information relating to munitions of war and communicating it to a foreign power, or communicating it in a manner that is prejudicial to the safety or interests of the state.
- [104] "Munitions of war" is defined in s. 2 of the SIA as arms, ammunition, implements or munitions of war, military stores or any articles capable of conversion into or use in the production of the above. "Communicate" is defined as including making available. "Foreign power" is defined as (a) the government of a foreign state; (b) an entity exercising the functions of a government outside Canada; or (c) a political faction or party operating within a foreign state whose purpose is to assume the role of government.
- [105] "Prejudicial to the safety or interests of the State" includes under s. 3(1)(g) and (h) conduct which "impairs or threatens the military capability of the Canadian Forces, or any part of the Canadian Forces" and "interfering with the design, development or production of any weapon, or defence equipment of, or intended for, the Canadian Forces, including any hardware, software or system that is part of or associated with any such weapon or defence equipment".
- [106] Counsel for Su argued there was no compelling evidence to suggest Co-con 1 and Co-con 2 were Chinese military offices or that they were acting on behalf of a foreign power. The Attorney General responded by pointing out that s. 4(2) of the SIA prohibits communicating directly or indirectly to a foreign power or communicating information "in any other manner prejudicial to the interests of the State".

[107] As stated, Col. Russell of the U.S. Air Force will testify the C-17, the F-35 and the F-22 aircraft were munitions of war and that communicating information pertaining to them was prejudicial to the interests of the U. S. There is also evidence both Co-con 1 and Co-con were members of the Chinese military, photographed in their military uniforms.

Conclusion

[108] In my view, the United States has met the test set out in s. 29(1) of the Act that a reasonable jury, properly instructed, could return a guilty verdict on the charges relied on in s. 342.1 of the Code and s. 4(2) of the SIA.

[109] The basis for my conclusion is that the ROC sets out the material examined by Customs and Border Protection Officer Masanto when Su entered the United States on December 31, 2012, including the contents of the form he submitted at the time and the business cards which he had with him naming Lode-Tech as a firm in which he was involved and providing the names of various email accounts associated with the business cards.

[110] The ROC lists the contents of many emails passing to and from those email accounts and the email addresses of persons named as Co-con1 and Co-con2 containing what is alleged to be highly sensitive information related to military aircraft which is alleged to be proprietary, password protected and confidential, and which originated from secure computers belonging to Boeing, Lockheed Martin, Excelis and Airbus, the manufacturers of the aircraft.

[111] I find the ROCs contain sufficient evidence to commit Su for trial in Canada and, therefore, I am satisfied that the United States has established a proper basis for committal of Su.

[112] Su is remanded into custody to await surrender on the offence specified in the ATP.

[113] By these reasons, Su is advised, pursuant to s. 38(2) of the Act that he will not be surrendered until after 30 days and that he has a right to appeal this order and to apply for judicial interim release.

"Greyell J."

Source & reproduction note

Judgment wording, source notices and original paragraph numbers are retained. Esheria supplies the layout and this PDF's page numbers; these are not the source pagination. This is a research copy, not an official or certified court document. Check quotations, citations and publication restrictions against the original source before relying on it.

ORIGINAL SOURCE <https://www.bccourts.ca/jdb-txt/SC/15/15/2015BCSC1586.htm>

CASE PAGE <https://chat.esheria.ai/case-law/canada/u-s-a-v-su-bin-2015-bcsc-1586>

Prepared on 29 October 2026 · Esheria