Supreme Court No. __________
Court of Appeals No. 47688-6-II

IN THE COURT OF APPEALS OF THE STATE OF WASHINGTON
DIVISION TWO

STATE OF WASHINGTON,
Plaintiff-Respondent,

v.

DAVID A. NOVICK,
Defendant-Appellant.

PETITION FOR REVIEW

By:
David B. Zuckerman
Attorney for Appellant
1300 Hoge Building
705 Second Avenue
Seattle, WA 98104
(206) 623-1595

TABLE OF CONTENTS

I. IDENTITY OF PETITIONER..1

II. COURT OF APPEALS DECISION...1

III. ISSUES PRESENTED FOR REVIEW..1

IV. STATEMENT OF THE CASE..1

V. ARGUMENT WHY REVIEW SHOULD BE ACCEPTED..............5

A. RAP 13.4(B) FAVORS REVIEW...5

B. MR. NOVICK SHOULD HAVE BEEN CHARGED WITH ONLY ONE COUNT EACH OF COMPUTER TRESPASS AND INTERCEPTING CONVERSATIONS BECAUSE THE CORRECT UNIT OF PROSECUTION COVERS THE ENTIRE COURSE OF CONDUCT..6

1. Legal Standards...6

2. The Computer Trespass Statute...7

3. Intercepting or Recording Private Conversations; RCW 9.73.030..12

VI. CONCLUSION...13

TABLE OF AUTHORITIES

Cases

Bell v. United States, 349 U.S. 81, 75 S.Ct. 620, 99 L.Ed. 905 (1955) 7

Ex parte Snow, 120 U.S. 274, 7 S.Ct. 556, 30 L.Ed. 658 (1887)................ 9

State v. Adel, 136 Wn.2d 629, 965 P.2d 1072 (1998)................................. 6

State v. David Novick, -- P.3d -- , 2016 WL 6216209 (Oct. 25, 2016) (Published Opinion).. 1, 10, 11

State v. Graham, 153 Wn.2d 400, 103 P.3d 1238 (2005)........................... 7

State v. Hall, 168 Wn.2d 726, 230 P.3d 1048 (2010)........................ passim

State v. Ose, 156 Wn.2d 140, 124 P.3d 635 (2005).................................... 7

Statutes

RCW 9.73.030 .... 12, 13

RCW 9A.52.110.. 7, 11

Rules

RAP 13.4.. 5, 6

I. IDENTITY OF PETITIONER

David Novick, through his attorney David Zuckerman, asks this Court to accept review of the Court of Appeals decision terminating review designated in Part II of this petition.

II. COURT OF APPEALS DECISION

On October 25 2016, Division Two of the Court of Appeals affirmed Mr. Novick's conviction and sentence. App. A; *State v. David Novick*, -- P.3d -- , 2016 WL 6216209 (Oct. 25, 2016) (Published Opinion).

III. ISSUES PRESENTED FOR REVIEW

1. What is the unit of prosecution for the crime of computer trespass?
2. What is the unit of prosecution for intercepting or recording private conversations?

IV. STATEMENT OF THE CASE

David Novick worked as an orthopedic trauma technician for Kaiser Permanente. 2B RP 592. In 2011 his wife Danielle Novick had an affair. 2B RP 578. Mr. Novick considered divorcing her, but ultimately the two of them agreed that they could both start seeing other people. The main condition was that that everything was in the open, including information on each other's cell phones. 2B RP 579-580. When Danielle found out that cell phones could track people, she thought that was a good idea and that would help build trust and safety. 2B RP 581. Around the beginning of 2012, they agreed to put software called Mobile Spy on all of their phones. 2B RP 581-82. That began in early 2012. 2B RP 582.

Mr. Novick viewed the software as essentially a "cloud" for all the data on the phone. When setting up the software, he clicked the boxes for every feature available. 2B RP 598. These included the option of obtaining audio and photographs from a remote phone. As far as Mr. Novick could tell these features acted randomly. He did not need to give any kind of command to receive data from his wife's phone. 2B RP 599. The program also served as a back-up for things like text messages. 2B RP 600. But Mobile Spy would only keep the data for a certain amount of time. *Id.* The text messages would come to him automatically about every hour through an email. 2B RP 601. Mr. Novick was not sure how long it would take stored information to disappear but thought it was approximately a week. 2B RP 603. He never reconfigured the phones.

Mr. Novick testified that he met Lisa Maunu through a dating website in December 2013. 2B RP 604. Because Ms. Maunu's old cell phone was not working well, Mr. Novick lent her his phone. 2B RP 607. When Ms. Maunu was unable to obtain her own Verizon account, Mr. Novick offered to put her on the account he shared with his wife. 2B RP 608. Mr. Novick ultimately gave Ms. Maunu his phone as a loan until she could get her own phone and account. 2B RP 610. Mobile Spy was still on the phone. *Id.* Mr. Novick obtained another phone for himself the next day. He promptly used "Google Play" to install all of the apps he had on his previous phone, including Mobile Spy. He set it up just like he used to. 2B RP 611. Then around March 11 or 12 Ms. Maunu was having trouble with the phone that Mr. Novick lent her so he lent her his new phone and bought another for himself. 2B RP 612. Again, he configured the phone with all his usual apps. 2B RP 613. He did not give much thought to having Mobile Spy on the phone he lent Ms. Maunu because he expected her to get her own phone soon. 2B RP 614. He was aware that Mobile Spy was sending him information from the phone in Ms. Maunu's possession, but for the most part he deleted that when it came in. 2B RP 614.

In her testimony Ms. Maunu agreed that her original phone was not working well. She maintained, however, that the Samsung Galaxy 4 phone that Mr. Novick ultimately gave her was a gift and not a loan. 1B RP 195-197, 202. Ms. Maunu became suspicious that something was wrong for two reasons: Mr. Novick seemed to know about things she had not yet told him and the phone started acting peculiarly. 1B RP 203-206; 211-213. On July 17, 2014, the phone completely stopped working. 1B RP 215. She then gave it back to Verizon. 1B RP 218-219.

Ms. Maunu ultimately contacted Kaiser with her suspicions that Mr. Novick was accessing her medical records. 1B RP 217-218. This led to an internal investigation by Daniel McManus and Robert Monsour, including a forensic review of computers Mr. Novick had access to. 1B RP 249-251. Mr. Monsour handled the forensic computer investigation. 1B RP 252-253. It turned out that Mr. Novick did not use Kaiser's system to access Ms. Maunu's records. But the investigation did reveal that Mr. Novick obtained information from Ms. Maunu's phone using Mobile Spy. 1B RP 259-260. Mr. McManus confirmed that Mr. Novick was using

Mobile Spy as early as June 2013, long before he met Ms. Maunu. 1B RP 267-68.

Mr. Monsour testified that a Kaiser employee has to log in to use a Kaiser computer, and then log in again to access its "Health Connect" system. 2A RP 358-359. The user can store information on a local computer or on his "P-Drive" (short for personal drive). The P-Drive is a folder on the server which allows a user to store information and then access it from any Kaiser computer. 2A RP 360. For purposes of this trial, Mr. Monsour focused on data on Mr. Novick's P-Drive on the dates of March 30, April 4, June 5, and June 6, 2014. 2A RP 387-388. Mr. Monsour identified several websites associated with Mobile Spy. 2A RP 384. The product had over a dozen features. 2A RP 397. Mr. Monsour learned that by the time of his investigation, Mobile Spy had removed two features: "surround recording" and "stealth camera." 2A RP 398.

All the charges in this case were based on the surround recording, which could cause a remote cell phone to turn on its audio recording feature. Mr. Monsour believed that a recording could take place only if the Mobile Spy user issued an affirmative command to record. 2A RP 414-420. The basis for that conclusion was quite flimsy. Although there was evidence that Mobile Spy did send some audio files to Mr. Novick, he insisted that this happened randomly with no control on his part. Mr. Monsour conceded that he never found any trace of a command to record audio. 2B RP 476-77.

The State charged Mr. Novick with eight counts of computer trespass in the first degree and eight counts of recording a private conversation. The element of intent to commit a crime elevated the trespass charges to first degree, a felony. CP 21-26. The only underlying crimes at issue were the counts of recording a private conversation, which are gross misdemeanors.

The jury convicted on all charges. CP 179-195. Mr. Novick was sentenced to 14 months on the trespass charges. The judge imposed 364 days on the recording charges, all of which were concurrent and suspended for 12 months. CP 211-225, 226-235.

V. ARGUMENT WHY REVIEW SHOULD BE ACCEPTED

A. RAP 13.4(B) FAVORS REVIEW

RAP 13.4(b)(1) applies because the Court of Appeals ruling conflicts with *State v. Hall*, 168 Wn.2d 726, 230 P.3d 1048 (2010). In *Hall*, this Court held that a continuing course of conduct gave rise to a single unit of prosecution. Mr. Novick's conduct was even more clearly a continuing course of conduct than Mr. Hall's, and nearly all the considerations in *Hall* apply as well to Mr. Novick's charges, yet the Court of Appeals found that Mr. Novick was properly convicted on eight counts.

RAP 13.4(b)(3) applies because convictions on excessive counts violate the double jeopardy provisions of the federal and state constitutions.

RAP 13.4(b)(4) applies because the Court of Appeals' published ruling was the first to decide the unit of prosecution for computer trespass and for intercepting private conversations. These rulings are now binding throughout the state. The validity of these rulings is a matter of substantial public interest that should be determined by the Supreme Court.

B. MR. NOVICK SHOULD HAVE BEEN CHARGED WITH ONLY ONE COUNT EACH OF COMPUTER TRESPASS AND INTERCEPTING CONVERSATIONS BECAUSE THE CORRECT UNIT OF PROSECUTION COVERS THE ENTIRE COURSE OF CONDUCT

1. Legal Standards

This Court's principles of statutory construction compel a finding that only one crime of each type was committed here.

"One aspect of double jeopardy protects a defendant from being punished multiple times for the same offense." *State v. Adel*, 136 Wn.2d 629, 632, 965 P.2d 1072, 1073 (1998). That protection is violated when a defendant is convicted on more counts than the unit of prosecution allows. *Id.* In *Adel*, as here, the defendant did not raise the double jeopardy issue at trial, but the constitutional challenge may be raised for the first time on appeal. *Id.* at 631-32. The Court of Appeals therefore reviewed this issue.

This Court set out the test for unit of prosecution most recently in *Hall*, 168 Wn.2d at 729. The first step is to analyze the statute in question. The Court then reviews the statute's history. "Finally we perform a factual analysis as to the unit of prosecution because even where the legislature has expressed its view on the unit of prosecution, the facts in a particular case may reveal more than one unit of prosecution is present." *Id.*[1] If the legislature "fails to define the unit of prosecution or its intent is unclear, under the rule of lenity any ambiguity must be resolved against turning a single transaction into multiple offenses." *Id.*[2] *See also*, *Bell v. United States*, 349 U.S. 81, 84, 75 S.Ct. 620, 99 L.Ed. 905 (1955). The standard of review is de novo. *State v. Ose*, 156 Wn.2d 140, 144, 124 P.3d 635, 636 (2005).

2. The Computer Trespass Statute

RCW 9A.52.110 reads in relevant part:

> **Computer trespass in the first degree.**
>
> A person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic database of another; and (a) The access is made with the intent to commit another crime.

On its face, the statute does not define the unit of prosecution. This Court, however, has emphasized that a statute's use of the definite article may shed light on the issue. *Ose*, 156 Wn.2d at 146-48. In *Ose*, the statute prohibited possession of "*a* stolen access device." (Emphasis added). The Court therefore concluded that the unit of prosecution was each stolen access device. *Id.* at 148. Similarly, in *State v. Graham*, 153 Wn.2d 400, 404, 103 P.3d 1238 (2005), the reckless endangerment statute required endangering "another." The Court considered "another" to be

[1] Citations and internal quotation marks omitted.

[2] Citations and internal quotation marks omitted.

equivalent to the definite article when referring to a person, and therefore concluded that the unit of prosecution was each person endangered.

The computer trespass statute uses both of these words. The person must gain access to "a" computer system or electronic database[3], and that computer must belong to "another." This suggests that there is a unit of prosecution for each computer trespassed upon and perhaps for each person to whom the computer belonged. Had the legislature intended each *trespass* to be a separate crime, however, it could have used different language, such as: "A person is guilty of *a* computer trespass in the first degree if, without authorization . . ." In this case the only computer at issue was the Galaxy 4 cell phone in Ms. Maunu's possession, and she testified that it belonged only to her. 1B RP 195-197, 202. Thus, on the facts of this case, the statutory language favors a single unit of prosecution.

The history of the statute does not shed any further light on this issue. The statute was enacted in 1984 and has never been amended. The legislative history does not include any discussion of the unit of prosecution.

However, in an analogous setting, a single unit of prosecution has been found to apply. In *Hall, supra,* the defendant was charged with four counts of witness tampering after he called the witness over 1,200 times in an effort to dissuade her from testifying against him. *Id.* 168 Wn.2d at

[3] For brevity, the statutory phrase "computer system or electronic database" will be referred to as "computer."

729. The Court noted that a unit of prosecution can be either an act or a "course of conduct." *Id.* at 731. This analysis goes back over 100 years. *See Hall*, 168 Wn.2d at 731, citing *Ex parte Snow*, 120 U.S. 274, 286, 7 S.Ct. 556, 30 L.Ed. 658 (1887) (bigamy is a single, ongoing offense). In *Hall*, "the course of conduct was continuous and ongoing, aimed at the same person, in an attempt to tamper with her testimony at a single proceeding." *Id.* at 736. The Court therefore found that the "offense is complete as soon as a defendant attempts to induce another not to testify or to testify falsely, whether it takes 30 seconds, 30 minutes, or days." *Id.* at 731. The defendant's crime may be considered a continuing course of conduct even if the legislature does not specifically use such terms in the statute. *Id.* at 733.

The same reasoning applies here. Mr. Novick was convicted of engaging in a single course of conduct with the single objective to spy on a single person's cell phone. He therefore committed only one count of computer trespass.

Further, in *Hall*, this Court noted that if each of the defendant's conversations were separate crimes that could lead to over 1,000 charges

> Such an interpretation could lead to absurd results, which we are bound to avoid when we can do so without doing violence to the words of the statute. It seems unlikely the legislature intended that a person could be prosecuted for over a thousand crimes under the circumstances presented here.

Hall, 168 Wn.2d at 737 (citations omitted).

That reasoning applies with greater force here. All (or in the State's view, most) of the trespasses were automated. Mobile Spy sent out information from Ms. Maunu's cell phone thousands of times within a few months. There were over 8,000 records involving the Mobile Spy websites, including at least 500 audio recordings. 2A RP 385. That is the nature of using computers to gather information. Once an automated program finds its way into an unauthorized computer, it can continue to access information indefinitely and at great speed. The legislature could not have intended to punish every access.

The Court of Appeals found sufficient evidence that all the computer trespass charges in this case were the result of Mr. Novick pressing a button. Published Opinion at 4-6. Even if that is true, however, there is no way to distinguish this case from *Hall*. Mr. Hall too had to push some buttons every time he placed a phone call to tamper with the witness. But that did not change the fact that he engaged in a single course of conduct.

Thus, under this Court's rules of statutory construction, Mr. Novick clearly should have been charged with only one count of computer trespass. In the alternative, if this Court finds that the unit of prosecution is unclear, it must nevertheless accept Mr. Novick's position under the rule of lenity.

The Court of Appeals rejected Mr. Novick's analysis regarding principles of statutory construction because it believed that the plain language of the statute clearly defined the unit of prosecution as one crime for each access of a computer. Published Opinion at 9. That position is untenable. The statute may be clear about what conduct is criminal, but it says nothing about the unit of prosecution. This aspect of the Court of Appeals ruling is particularly troubling. If the statute unambiguously requires a separate crime for every unlawful access, then the run-of-the-mill computer trespass case will often involve thousands or millions of crimes. The Court of Appeals' approach leaves no possibility for a single course of conduct under any circumstances.

The Court of Appeals' conclusion seems to be based in part on a misunderstanding of *Hall.*

> The operative criminal act prohibited by former RCW 9A.52.110 is the unauthorized access to another's computer. Stated another way, the "evil the legislature has criminalized" is the access. See *Hall*, 168 Wn. 2d at 731; RCW 9A.52.110. The violation of the statute is complete as soon as the defendant accesses another's computer system with the intent to commit a crime.

Published Opinion at 9-10.

Mr. Novick agrees with that statement. But it compels the opposite conclusion. As *Hall* explained, that the violation is complete after a single transgression implies that the unit of prosecution is one.

> [Hall] argues the evil the legislature has criminalized is the attempt to "induce a witness" not to testify or to testify falsely. The *number* of attempts to "induce a witness" is secondary to that statutory aim, which centers on interference with "a witness" in "any official proceeding" (or investigation). RCW 9A.72.120(1).The offense is complete as soon as a defendant attempts to induce another

> not to testify or to testify falsely, whether it takes 30 seconds, 30 minutes, or days. We agree.

Hall, 168 Wn.2d at 731.

3. Intercepting or Recording Private Conversations; RCW 9.73.030

The analysis for this statute is similar to that for the Computer Trespass charges. Again, the unit of prosecution is an issue of first impression. The statute reads in relevant part:

> (1) Except as otherwise provided in this chapter, it shall be unlawful for any individual, partnership, corporation, association, or the state of Washington, its agencies, and political subdivisions to intercept, or record *any*: . . .
>
> (b) Private conversation, by any device electronic or otherwise designed to record or transmit such conversation regardless how the device is powered or actuated without first obtaining the consent of all the persons engaged in the conversation.

(Emphasis added). The word "any" has several meanings, but none of them are restricted to the singular. The most natural meaning of the word in this context is "one or more – used to indicate an undetermined number or amount." *Merriam-Webster online dictionary.*[4] Had the legislature intended the unit of prosecution to be each conversation, it would have used the definite article "a."

The history of the statute is not helpful. The statute was first enacted in 1967 and there have been some minor changes since then, but none that shed light on the unit of prosecution.

[4] http://www.merriam-webster.com/dictionary/any

As with the witness tampering charges addressed in *Hall*, and the computer trespass charges discussed above, the violation of RCW 9.73.030 should be treated as a continuing course of conduct, at least on the facts of this case. Assuming that the State's theory of the case is correct, recording conversations was just one aspect of Mr. Novick's single objective to continuously spy on Ms. Maunu. Over 400 audio recordings were involved. 2A RP 321. Again, even if the legislature's intent is not clear, the rule of lenity requires this Court to accept Mr. Novick's position.

VI. CONCLUSION

Computer crime has become increasingly prevalent since the statutes at issue here were first enacted. It is essential for this Court to definitively rule on how such crimes should be prosecuted. The Court should therefore accept review.

DATED this 18th day of November, 2016.

Respectfully submitted,

David B. Zuckerman, WSBA #18221
Attorney for David Novick

CERTIFICATE OF SERVICE

I hereby certify that on the date listed below, I served by email and United States Mail, postage prepaid, one copy of the foregoing Petition for Review on the following:

Ms. Rachael Probstfeld
Clark County Prosecutor's Office
PO Box 5000
Vancouver, WA 98666-5000
Email: CntyPA.GeneralDelivery@clark.wa.gov

11/18/2016
Date

Peyush
Peyush Soni

Filed
Washington State
Court of Appeals
Division Two

October 25, 2016

IN THE COURT OF APPEALS OF THE STATE OF WASHINGTON

DIVISION II

STATE OF WASHINGTON, Respondent, v. DAVID A. NOVICK, Appellant.	No. 47688-6-II PUBLISHED OPINION

WORSWICK, J. — David Novick appeals his convictions for eight counts of first degree computer trespass and eight counts of recording private communications after he installed a spying application on his girlfriend's mobile phone. Novick argues that the State failed to provide sufficient evidence that he intentionally recorded a private communication. Novick also argues that entry of eight convictions of each crime violated his right against double jeopardy because the correct unit of prosecution covers the entire course of conduct. We disagree and affirm Novick's convictions.

FACTS

David Novick and Lisa Maunu began dating in December 2013. At the beginning of their relationship, Maunu used an old mobile phone. When Maunu's phone started to malfunction, Novick bought her a new mobile phone on March 11, 2014, and set it up for her.

Unbeknownst to Maunu, Novick had installed an application called Mobile Spy on Maunu's new phone. The application allowed a person to log onto the Mobile Spy website and monitor the phone on which the application was installed. From the Mobile Spy website, a user could access all the information stored on the monitored phone, including text messages, call logs, and e-mails. The versions of Mobile Spy used on Maunu's phone, versions 6.5 and 6.6, also permitted a user to send commands to the phone from a "live control panel" on the website. Verbatim Report of Proceedings (VRP) at 416. One such command allowed a user to activate the phone's microphone and recording feature and record audio into a file that could then be downloaded from the website.

In July, the relationship between Novick and Maunu soured, and Maunu noticed that her new phone was acting strangely. The phone would light up periodically, send text messages and emails without her knowledge, and frequently "lock up." VRP at 212. About the same time, Maunu became concerned because Novick expressed specific knowledge about Maunu's health conditions, medications, doctors' appointments, and private conversations. Maunu then contacted Kaiser Permanente, where she received her health care and also where Novick worked, because she was concerned Novick was accessing her medical records at his work.

A compliance investigator for Kaiser ordered a forensic review of Novick's work computer use. The forensic review was conducted by Robert Monsour. During his investigation, Monsour reviewed the records associated with Novick's password-protected user account. Kaiser computers keep records of every URL[1] visited on an employee's work computer and the date and time of each visit. Monsour found a pattern of Novick accessing websites associated with Mobile Spy from Novick's computer account at Kaiser. In addition to the

[1] "Uniform resource locator" (URL) is a protocol for specifying the "addresses of the webpage." VRP at 366.

Mobile Spy websites, Monsour found evidence that Novick had downloaded over 500 audio files from Mobile Spy, searched for GPS (global positioning system) locations, and searched for particular telephone numbers.

The State charged Novick with eight counts of first degree computer trespass[2] and eight counts of recording private communications[3] based on Novick's use of Mobile Spy to record Maunu's conversations on March 30, April 4, June 5, and June 6.[4]

During trial, Monsour testified about his investigation into Novick's computer records. To understand how Mobile Spy operated, Monsour read all of the available documentation, focusing on versions 6.5 and 6.6—the versions of Mobile Spy available on the dates in question.[5] Monsour also explored an available demo feature of version 7.01 of the program. Version 7.01 of Mobile Spy removed the surround recording feature, among other slight variations.

According to the user guides Monsour read, in order to begin a recording through Mobile Spy, a user had to go to a "live control panel" on their website and affirmatively send a command through the control panel to the monitored phone. Monsour described the process as similar to "pushing a record button on a tape recorder but you're able to do it from anywhere

[2] Former RCW 9A.52.110 (1984), repealed by LAWS OF 2016 ch. 164, § 14.

[3] RCW 9.73.030.

[4] On those 4 days, Novick downloaded 19 separate audio recordings from Maunu's phone, capturing various conversations between Maunu and her neighbor, a friend, her mother, and Novick himself.

[5] The phone Novick installed Mobile Spy on was unavailable for investigation because Maunu exchanged her malfunctioning mobile phone before discovering the spying application.

where you can get on the internet." VRP at 416. In an attempt to confirm this process for beginning a recording, Monsour contacted Mobile Spy's technical support. Monsour asked the technical support staff whether a recording had to be started manually or if there was some way to automate it so the phone would keep recording repeatedly. The technical support staff confirmed that a user had to manually start a recording every time.

Novick testified on his own behalf. Novick acknowledged his extensive use of Mobile Spy, but he contended that everything on Mobile Spy—including the surround recording feature—occurred automatically at random times.

The jury trial found Novick guilty of all counts as charged. Novick appeals.

ANALYSIS

I. Sufficiency of the Evidence

Novick argues that the evidence was insufficient to support any of his convictions. He contends that because the application automatically recorded conversations, the State failed to provide sufficient evidence that Novick intentionally recorded private communications. Viewing the evidence in the light most favorable to the State, we hold that sufficient evidence exists to support Novick's convictions. *State v. Hosier*, 157 Wn.2d 1, 8, 133 P.3d 936 (2006).

Sufficient evidence supports a conviction if, when viewed in the light most favorable to the State, any rational trier of fact could have found the essential elements of the charged crime proved beyond a reasonable doubt. *Hosier*, 157 Wn.2d at 8. We draw all reasonable inferences from the evidence in favor of the State and interpret them most strongly against the defendant. *Hosier*, 157 Wn.2d at 8. When reviewing evidence for sufficiency, circumstantial evidence and direct evidence carry equal weight. *State v. Goodman*, 150 Wn.2d 774, 781, 83 P.3d 410 (2004). We defer to the fact finder on issues of conflicting testimony, witness credibility, and persuasiveness of the evidence. *State v. Thomas*, 150 Wn.2d 821, 874-75, 83 P.3d 970 (2004).

First degree computer trespass occurs when a person intentionally gains access without authorization to a computer system or electronic database of another and the access is made with the intent to commit another crime. Former RCW 9A.52.110 (2011), repealed by LAWS OF 2016 ch. 164, § 14. Here, the underlying crime was recording private communications. A person commits the crime of recording private communications when he intercepts or records private communications transmitted by any device designed to record and/or transmit said communications. RCW 9.73.030.

Novick contends that the evidence is insufficient to prove he issued a command to begin audio recording from the live control panel because the computer records did not explicitly show Novick issued a command. To support his claim, Novick relies on his own refuted testimony that Mobile Spy automatically recorded the communications without a command to do so. Assuming without deciding that proof of manual commands is required to establish sufficient evidence, such proof existed. Monsour accounted for the absence of specific computer records showing a manual command was given by explaining that the records show only the activity that resulted in a new URL, and that commands could be sent within an internet program without creating a new URL.

The forensic review of Novick's computer activity revealed substantial circumstantial evidence that Novick sent the commands. Monsour testified that "every bit of information" confirmed that in order to activate the surround recording feature of the Mobile Spy program, a user must visit the Mobile Spy website and send a command through the program's live control panel. VRP 398. And the computer records showed that Novick visited the live control panel on Mobile Spy's website and subsequently downloaded audio files.

Novick characterizes the State's evidence that Novick issued commands to record from the live control panel as "flimsy" and "weak." Br. of Appellant 10, 12. But we defer to the trier of fact on issues of conflicting testimony, credibility of witnesses, and the persuasiveness of the evidence. *Thomas*, 150 Wn.2d at 874-75. The conflicting testimony from Novick and Monsour created a credibility determination, which we leave to the trier of fact. *State v. Miller*, 179 Wn. App. 91, 105, 316 P.3d 1143 (2014).

Viewed in the light most favorable to the State, the evidence supports a finding that Novick sent commands from the live control panel to intentionally record Maunu's private communications. Accordingly, we hold that the State presented sufficient evidence for a rational jury to conclude beyond a reasonable doubt that Novick committed the crime of recording private communications, and thus committed computer trespass.

II. Double Jeopardy And Unit of Prosecution

Novick argues in the alternative that his multiple convictions for computer trespass and recording private communications violate the prohibition against double jeopardy because the correct unit of prosecution for each crime covers the entire course of Novick's conduct. We disagree.

The Fifth Amendment to the United States Constitution provides that no "person be subject for the same offense to be twice put in jeopardy of life or limb." Similarly, article I, section 9 of the Washington Constitution provides, "No person shall . . . be twice put in jeopardy for the same offense." These double jeopardy provisions prohibit, among other things, multiple convictions for the same offense. *State v. Hall*, 168 Wn.2d 726, 729-30, 230 P.3d 1048 (2010). We review double jeopardy claims de novo. *State v. Villanueva-Gonzalez*, 180 Wn.2d 975, 979-80, 329 P.3d 78 (2014).

"When a defendant is convicted for violating one statute multiple times, the proper inquiry is 'what unit of prosecution has the Legislature intended as the punishable act under the specific criminal statute.'" *State v. Reeder*, 184 Wn.2d 805, 825, 365 P.3d 1243 (2015) (internal quotations omitted) (quoting *State v. Adel*, 136 Wn.2d 629, 634, 965 P.2d 1072 (1998)). In such a case, we determine whether there is a double jeopardy violation by asking, "'What act or course of conduct has the Legislature defined as the punishable act?'" *State v. Boswell*, 185 Wn. App. 321, 327, 340 P.3d 971 (2014), *review denied*, 183 Wn.2d 1005 (2015) (quoting *Villanueva-Gonzalez*, 180 Wn.2d at 980). The scope of the criminal act as defined by the legislature is considered the unit of prosecution. *Reeder*, 184 Wn.2d at 825. "The issue is one of statutory interpretation and legislative intent." *Reeder*, 184 Wn.2d at 825.

The first step is to analyze the statute in question. *State v. Jensen*, 164 Wn.2d 943, 949, 195 P.3d 512 (2008). If the statute does not plainly define the unit of prosecution, we next examine the legislative history to discern legislative intent. *Jensen*, 164 Wn.2d at 949. Finally, we perform a factual analysis to determine if, under the facts of the specific case, more than one unit of prosecution is present. *Hall*, 168 Wn.2d at 735. If the legislature fails to define the unit of prosecution or its intent is unclear, any ambiguity must be resolved against allowing a single incident to support multiple convictions. *State v. Tvedt*, 153 Wn.2d 705, 711, 107 P.3d 728 (2005).

A. *The Plain Language of the Statutes*

When interpreting a statute, our fundamental objective is to determine and give effect to the legislature's intent. *State v. Larson*, 184 Wn.2d 843, 848, 365 P.3d 740 (2015). We look first to the statute's plain language to determine this intent. *Larson*, 184 Wn.2d at 848. We discern the plain meaning of a statutory provision from the ordinary meaning of the language at issue, as well as from the context of the statute in which that provision is found, related provisions, and the statutory scheme as a whole. *State v. Polk*, 187 Wn. App. 380, 389, 348 P.3d 1255 (2015). We avoid a reading that produces absurd results because we presume that the legislature does not intend absurd results. *State v. Delgado*, 148 Wn.2d 723, 733, 63 P.3d 792 (2003).

In applying the unit of prosecution analysis, courts look to discern "the evil the legislature has criminalized." *Hall*, 168 Wn.2d at 731. The focus of this court's inquiry is on the actual *act* necessary to commit the crime. *Boswell*, 185 Wn. App. at 329.

"A person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic database of another; and (a) the access is made with the intent to commit another crime." Former RCW 9A.52.110. "Access" as charged here means to "approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, directly or by electronic means." RCW 9A.52.010(1) (2011).

A person is guilty of recording private communication when he "intercept[s], or record[s] any":

> (a) Private communication transmitted by telephone . . . or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication;
>
> (b) Private conversation, by any device electronic or otherwise designed to record or transmit such conversation regardless how the device is powered or actuated without first obtaining the consent of all the persons engaged in the conversation.

RCW 9.73.030(1).

Novick contends that the language used in the statutes "suggests that there is a unit of prosecution for each computer trespassed upon and perhaps for each person to whom the computer belonged."[6] Br. of Appellant 15. The State responds that the plain language of the statutes define the proper unit of prosecution as each time a person gains unauthorized access to a computer and each conversation recorded without consent. We agree with the State.

The operative criminal act prohibited by former RCW 9A.52.110 is the unauthorized access to another's computer. Stated another way, the "evil the legislature has criminalized" is the access. See *Hall*, 168 Wn.2d at 731; RCW 9A.52.110. The violation of the statute is

[6] Novick does not state what he believes to be the proper unit of prosecution for recording private communication, rather he simply rejects the State's interpretation that the unit of prosecution is each recorded conversation.

complete as soon as the defendant accesses another's computer system with the intent to commit a crime. Likewise, RCW 9.73.030 prohibits recording private conversation without the consent of each participant in that conversation.

Novick contends that had the legislature intended each trespass, as opposed to each computer system, to be a separate crime it could have used such language as "a person commits *a* computer trespass in the first degree if. . . ." Br. of Appellant 15. Likewise he contends that had the legislature intended the unit of prosecution for recording private communication to be each conversation, it could have used the language "by recording . . . a private conversation."

To support his argument, Novick relies on *State v. Ose*, 156 Wn.2d 140, 124 P.3d 635 (2005). There, our Supreme Court held that by using the indefinite article "a" in the clause "possesses a stolen access device" the legislature unambiguously defined the unit of prosecution for possessing stolen property, as defined by RCW 9A.56.160(1)(c),[7] as one count per stolen access device. *Ose*, 156 Wn.2d at 146. Novick attempts to analogize the court's interpretation in *Ose* to the first degree computer trespass statute by focusing on the statute's use of "*a* computer system or electronic database." Br. of Appellant at 15. However, Novick's analogy is not persuasive.

Novick is correct that the legislature's use of the word "a" in a criminal statute *may* authorize punishment for each individual instance of criminal conduct even when the conduct occurs simultaneously. *Ose*, 156 Wn.2d at 147. However, *Ose* does not stand for the converse

[7] RCW 9A.56.160(1)(c) provides: "A person is guilty of possessing stolen property in the second degree if . . . [h]e or she possesses a stolen access device."

proposition that the article "a" anywhere in a statute is *required* to define one unit of prosecution. Rather, we look at the statute as a whole to discern the criminal act the legislature intended to prohibit. We are not persuaded by Novick's argument that if the legislature intended a single unit of prosecution based on a course of conduct, it could have said so plainly. What matters is not what the legislature did not say, but what it did say. *State v. Vidales Morales*, 174 Wn. App. 370, 387, 298 P.3d 791 (2013).

The better analogy is to *State v. Brooks*, 113 Wn. App. 397, 400, 53 P.3d 1048 (2002), where Division One of our court determined the unit of prosecution for the crime of burglary by focusing on the action prohibited by the statute—unlawfully entering or remaining in a building—rather than the number of victims. Similarly, in *State v. Allen*, 150 Wn. App. 300, 314, 207 P.3d 483 (2009), we focused on the action prohibited by the violation of a no-contact order statute when we held that the defendant could properly be charged with two violations of a no-contact order for sending two e-mails on different days that the victim viewed at the same time.

Novick further argues that the State's interpretation of the units of prosecution would lead to absurd results. He contends that by defining the unit of prosecution for computer trespass as every access, the State could charge an unlimited number of counts based on the automated access of a program into a computer system. But the charges at issue here are specifically limited to Novick's use of the live control panel to record and download Maunu's private conversations. Whether Novick's specific actions in this case constitute separate and distinct acts of computer trespass is a factual question we decide separately from determining the unit of prosecution intended by the legislature.

The plain language of the statutes support the conclusion that the units of prosecution for first degree computer trespass and recording private communication are each separate unauthorized access and each recording of a conversation without consent.

B. *Novick's Actions Constituted More Than One Unit of Prosecution*

Once the unit of prosecution is determined, we next conduct a factual analysis to decide if more than one unit of prosecution exists. *Hall*, 168 Wn.2d at 735. The essential question is whether Novick committed separate crimes with each access and each recording. Factors that can be considered in addressing whether each act is a separate or distinct violation include the method used to commit the crime; the amount of time between the acts; and whether the initial conduct was interrupted, failed, or abandoned. *See Boswell*, 185 Wn. App. at 332.

Novick argues that his actions constituted "a single course of conduct with the single objective to spy on a single person's cell phone," and therefore, he should have been charged with only one count of each crime. Br. of Appellant at 16. We disagree.

Both Novick and the State cite *Hall*, 168 Wn.2d 726, to support their argument. In *Hall*, the defendant was convicted of 3 counts of witness tampering after attempting to call one witness over 1,200 times within 3 days to convince her not to testify against him. *Hall*, 168 Wn.2d at 729. Our Supreme Court explained that "'[t]he obstruction of justice is the evil which the statute was designed to forestall,'" and therefore, the *number* of attempts was secondary to that purpose. *Hall*, 168 Wn.2d at 735 (quoting *State v. Stroh*, 91 Wn.2d 580, 582, 588 P.2d 1182 (1979)). The court held that because the defendant's conduct in that case was continuous, aimed at a single person, and meant to tamper with her testimony in a single proceeding, there was only one violation of the statute. *Hall*, 168 Wn.2d at 736. The Supreme Court noted that their determination may have been different had the defendant changed his strategy, or if he had briefly stopped his witness tampering before resuming it again at a later time. *Hall*, 168 Wn.2d at 737.

State v. Kinneman, 120 Wn. App. 327, 84 P.3d 882 (2003), addressed a similar issue. There, Kinneman made 67 unauthorized withdrawals from an individual's trust account. *Kinneman*, 120 Wn. App. at 327. The State charged Kinneman separately for each withdrawal resulting in 28 counts of first degree theft and 39 counts of second degree theft. Kinneman argued that his numerous withdrawals constituted only a single count of first degree theft because all the takings were from the same place and the same victim. *Kinneman*, 120 Wn. App. at 334. Division One of this court rejected Kinneman's argument, holding that each separate withdrawal occurring at different times could be viewed as a distinct theft. *Kinneman*, 120 Wn. App. at 338.

The facts of this case are similar to *Kinneman*. While Novick's actions were somewhat repetitious, they were not continuous. On at least eight separate and distinct times, Novick logged onto Mobile Spy's website, accessed Maunu's phone by issuing a command through the live control panel, and downloaded at least eight different recordings of conversations between Maunu and various other people. Each access was separated by time and reflected a separate intent to record a separate conversation.

We hold that Novick's eight convictions for first degree computer trespass and eight convictions for recording private conversations do not violate double jeopardy principles because he was not charged multiple times for the same offense. Each count was based on evidence of eight distinct times that Novick's conduct violated each statute.

CONCLUSION

We hold that the State provided sufficient evidence that Novick intentionally recorded eight private communications. Additionally, Novick's actions constituted multiple units of prosecution, and therefore, his multiple convictions did not violate double jeopardy principles. Thus, we affirm Novick's convictions.

Worswick J
Worswick, J.

We concur:

Maxa, A.C.J.
Maxa, A.C.J.

Melnick J.
Melnick, J.

DAVID ZUCKERMAN LAW OFFICE

November 21, 2016 - 4:41 PM

Transmittal Letter

Document Uploaded: 3-476886-Petition for Review~2.pdf

Case Name: State of Washington v. David A. Novick

Court of Appeals Case Number: 47688-6

Is this a Personal Restraint Petition? Yes ● No

The document being Filed is:

Designation of Clerk's Papers   Supplemental Designation of Clerk's Papers

Statement of Arrangements

Motion: ____

Answer/Reply to Motion: ____

Brief: ____

Statement of Additional Authorities

Cost Bill

Objection to Cost Bill

Affidavit

Letter

Copy of Verbatim Report of Proceedings - No. of Volumes: ____
Hearing Date(s): ________

Personal Restraint Petition (PRP)

Response to Personal Restraint Petition

Reply to Response to Personal Restraint Petition

● Petition for Review (PRV)

Other: ________

Comments:

After filing a copy of the Petition for Review in this matter on November 18, 2016 via the electronic portal, Appellant realized that he inadvertently forgot to attach Appendix A (the copy of the Court of Appeals Opinion that is to be reviewed), to the copy that was filed. After calling the Washington State Supreme Court Clerk's Office, the Clerk recommended another version be filed with no other changes than to attach the missing attachment. To summarize, the only attachment on this copy is the inclusion of attachment A, which was accidentally left out in the initial filing.

Sender Name: David Zuckerman - Email: peyush@davidzuckermanlaw.com

A copy of this document has been emailed to the following addresses:

CntyPA.GeneralDelivery@clark.wa.gov