

NO. 47688-6-II

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

STATE OF WASHINGTON, Respondent

v.

DAVID A NOVICK, Appellant

FROM THE SUPERIOR COURT FOR CLARK COUNTY
CLARK COUNTY SUPERIOR COURT CAUSE NO.14-1-01698-1

BRIEF OF RESPONDENT

Attorneys for Respondent:

ANTHONY F. GOLIK
Prosecuting Attorney
Clark County, Washington

RACHAEL R. PROBSTFELD, WSBA #37878
Senior Deputy Prosecuting Attorney
Office ID No. 91127

Clark County Prosecuting Attorney
1013 Franklin Street
PO Box 5000
Vancouver WA 98666-5000
Telephone (360) 397-2261

TABLE OF CONTENTS

RESPONSE TO ASSIGNMENTS OF ERROR 1

 I. There was sufficient evidence to support Novick’s convictions.
 1

 II. Double Jeopardy does not bar multiple convictions for
 computer trespass and intercepting, recording or divulging a
 private communication. 1

STATEMENT OF THE CASE 1

ARGUMENT 7

 I. There was sufficient evidence to support Novick’s convictions.
 7

 II. Double Jeopardy does not bar multiple convictions for
 computer trespass and intercepting, recording or divulging a
 private communication. 9

CONCLUSION..... 14

TABLE OF AUTHORITIES

Cases

<i>Bell v. United States</i> , 349 U.S. 81, 75 S. Ct. 620, 99 L. Ed. 905 (1955) ..	10
<i>Harrell v. State</i> , 88 Wis. 2d 546, 277 N.W.2d 462, 469 (1979).....	13
<i>State v. Adel</i> , 136 Wn.2d 629, 965 P.2d 1072 (1998).....	10
<i>State v. Calle</i> , 125 Wn.2d 769, 888 P.2d 155 (1995)	10
<i>State v. Chouap</i> , 170 Wn. App. 114, 285 P.3d 138 (2012).....	12
<i>State v. Elliott</i> , 114 Wn.2d 6, 785 P.2d 440 (1990).....	10
<i>State v. Gocken</i> , 127 Wn.2d 95, 896 P.2d 1267 (1995).....	10
<i>State v. Green</i> , 94 Wn.2d 216, 616 P.2d 628 (1980).....	8
<i>State v. Hall</i> , 168 Wn.2d 726, 230 P.3d 1048 (2010).....	12, 13
<i>State v. Mason</i> , 31 Wn.App. 680, 644 P.2d 710 (1982)	10
<i>State v. Salinas</i> , 119 Wn.2d 192, 829 P.2d 1068 (1992)	8
<i>State v. Tili</i> , 139 Wn.2d 107, 985 P.2d 365 (1999).....	10, 13

Statutes

RCW 9.73.030	8, 11
RCW 9A.52.110.....	8, 11

Constitutional Provisions

Const. art. I, § 9.....	10
U.S. Const. amend. V.....	10

RESPONSE TO ASSIGNMENTS OF ERROR

- I. **There was sufficient evidence to support Novick's convictions.**
- II. **Double Jeopardy does not bar multiple convictions for computer trespass and intercepting, recording or divulging a private communication.**

STATEMENT OF THE CASE

David Novick was charged with eight counts of Computer Trespass in the First Degree and eight counts of Intercepting, Recording or Divulging a Private Communication for incidents involving Novick putting spyware on his girlfriend's cell phone and accessing the microphone and text message system of the cell phone without her knowledge or permission. CP 11-16. Novick was convicted of all 16 counts, with special allegations on each count that this involved domestic violence. CP 179-95.

The evidence at trial showed that Lisa Maunu met Novick on December 12, 2013 through an online dating website called Plenty of Fish. RP 184. Novick told Ms. Maunu that he was unmarried and had no children. RP 185. They began a dating relationship. RP 184-85. Ms. Maunu and Novick dated for six or seven months. RP 187-88. At the time, Novick worked for Kaiser Health Systems. RP 189.

When Novick and Ms. Maunu started dating, Ms. Maunu had a basic flip phone cell phone. RP 190. She was not interested in technology. *Id.* Ms. Maunu was happy with her phone and didn't want a new phone. RP 191. However, Novick really wanted her to have a new phone because hers was old and wasn't working perfectly and Ms. Maunu couldn't always respond quickly to Novick. RP 191-92, 196. Novick bought Ms. Maunu a phone as a gift from Verizon in March 2014. RP 192. The IMEI¹ on the phone Novick bought for her was 990004425520701. RP 196. Ms. Maunu paid for the cell phone access plan. RP 202.

Novick set up the phone for Ms. Maunu, including setting up her email, text messaging, Facebook, etc. RP 197. Whenever the phone acted weird or needed an update or anything Ms. Maunu didn't understand she would hand the phone to Novick and he would do something on her phone. RP 199.

Ms. Maunu never gave Novick permission to download spyware onto her phone and she did not know he had done so. RP 200. She never gave him permission to access her phone remotely, nor did she give him permission to access her conversations over the phone. RP 200-01.

Ms. Maunu broke up with Novick in July 2014 and she wanted no further contact from him. RP 211. Ms. Maunu became suspicious when

¹ International Mobile Equipment Identity

Novick knew information about her health that she had not disclosed to him, so she believed he was using his access at Kaiser to access her medical records, or that he was doing something through her cell phone. RP 211-12, 218. Ms. Maunu's cell phone was behaving oddly and then one day in July 2014 it locked and she could not access it. RP 214. She went to the Verizon store to try to have it unlocked, but they were unable to. RP 214-15. Ms. Maunu gave the phone to Verizon and got a new phone. RP 215. Ms. Maunu reported to Kaiser her suspicions and she spoke with Daniel McManus, one of the Kaiser detectives. RP 219.

Witness Daniel McManus testified for the State that he worked as a compliance investigator for Kaiser, investigating allegations of violations of Kaiser's policies. RP 248. He received a complaint regarding Novick that his ex-girlfriend, Ms. Maunu, was concerned about him accessing protected healthcare information from Kaiser's internal system. RP 249. As part of his investigation he requested a forensic review of Novick's work computer. RP 251. A different department conducts this type of forensic review. RP 251. He also requested an audit of records accessed by Novick. RP 252. Mr. McManus found that Novick had not accessed Ms. Maunu's healthcare records. RP 253. Mr. McManus was in frequent contact with Mr. Monsour, the person conducting the forensic review of Novick's computer. *Id.*

As part of his investigation Mr. McManus met with Novick and asked him if he had ever used a Kaiser computer to access a cell phone monitoring program such as Mobile Spy. Novick admitted he had done so. RP 259-60. Novick also told him he started using the program in March 2014, and would access the browser window to monitor the cell phones. RP 259-60. Novick also admitted to downloading audio files from the cell phones onto his work computer. RP 261-63. Mr. McManus identified 69 dates that Novick had accessed Mobile Spy and Karen Eckardt, Novick's supervisor at Kaiser, confirmed that Novick worked on 69 dates that were provided to her by Mr. McManus. RP 276.

Witness Robert Monsour is a digital forensic investigator for Kaiser Permanente. RP 346. He testified that malware is a spyware program that is designed to allow someone to gain unauthorized access to a computer system. RP 348. Every Kaiser employee has his or her own username and a password he or she chooses in order to access the computer system. RP 357-59. Mr. Monsour has the ability to tell the date and time that a user does something on a computer, such as access the internet and download files. RP 362, 370.

In reviewing this case, Mr. Monsour found over a thousand records of visits to websites from Novick's user name on March 30, April 4, June 5 and June 6, 2014. RP 383-84. Mr. Monsour found thousands of visits to

a mobile spy website, with over 400 audio downloads and activity searching for GPS locations. RP 385. Mr. Monsour found activity under Novick's log in involving Mobile Spy on 69 different dates. RP 392.

Mr. Monsour learned all he could about the Mobile Spy program by reading all of the user documentation available, used the program's online demo feature, and spoke with Mobile Spy's technical staff. RP 395-97. The program is one an individual can install on a cell phone that he or she wants to monitor and then go to any computer and log into a Mobile Spy account and see everything that's going on with the phone and manually perform certain things, like recording, taking photographs, etc. RP 403. Mr. Monsour used the online demo to see how the Mobile Spy program worked. RP 403. On top of being able to record anything being said in the vicinity of the cell phone, or seeing through the camera lens on the phone, you can see and read all text messages, email messages, etc. coming into and out of the cell phone. RP 403-04.

Mobile Spy has a live control panel where the user can send commands directly to the cell phone which make the phone do certain things. RP 414. For the recording option, the program works essentially like pushing a record button on a tape recorder: you go to the live control panel on a computer and send a command to the cell phone and that starts the phone's recorder. RP 416. Every time you want to record what is

happening around the cell phone, the user has to go manually start the recording. RP 416.

One feature of Mobile Spy was called 'surround recording.' It allowed someone to install it on a cell phone and then go to a website from a computer and command it to start recording and the cell phone's microphone then would start recording anything that it could pick up. RP 398. This feature stopped being offered by Mobile Spy in September or October 2014, but was offered on the version Novick had downloaded. RP 398-99. Another feature of Mobile Spy is called 'stealth camera.' RP 399. This feature allows you to put it on a cell phone and take a picture of what the cell phone's camera is showing without the person who possesses the cell phone knowing what is happening. RP 399. This feature also stopped being offered by Mobile Spy. RP 399.

The first time Novick ever accessed the Mobile Spy website from his work computer was March 12, 2014. RP 422. Exhibit 15 is an audio CD of the recordings of conversations overheard from Ms. Maunu's cell phone. One is from March 30, 2014 at 4:32 p.m. Another, on March 30, 2014 at 4:38 p.m., is of the same two women discussing medical issues and sexual issues. RP 442-44. On March 30, 2014 at 4:52 p.m. the computer records showed another conversation was downloaded from the Mobile Spy website. RP 445-46. Novick downloaded a third audio file of

a conversation on March 30, 2014 at 5:53 p.m. RP 451. On April 4, 2014, computer records show Novick accessed and downloaded an audio call wherein the woman identified as Lisa receives a phone call and talks on the phone. RP 456. On June 5, 2014, Novick accessed and downloaded audio files of conversations. RP 463-64. He downloaded another audio file of a recorded conversation on June 6, 2014. RP 464.

Ms. Maunu testified that all the recordings on Exhibit 15 were private conversations between herself and others that Novick did not have permission to access, that she did not know he accessed and that she did not give consent for him to intercept or record. RP 518-53. These included conversations about her health issues, a friend's health issues, her sex life, a friend's autistic child, etc. *Id.* Ms. Maunu testified that most of these were highly private conversations. *Id.* She testified she was in Vancouver for these conversations. *Id.*

ARGUMENT

I. There was sufficient evidence to support Novick's convictions.

Novick argues the evidence is insufficient to support his convictions for Computer Trespass in the First Degree and Interception of a Private Communication. When viewed in the light most favorable to the

State, there is more than sufficient evidence that he committed these crimes. Novick's claim fails.

When reviewing a claim of insufficiency, the Court of Appeals must determine whether, when viewing the evidence in the light most favorable to the State, any rational trier of fact could have found the elements of the offense beyond a reasonable doubt. *State v. Green*, 94 Wn.2d 216, 221, 616 P.2d 628 (1980). A challenge to the sufficiency of the evidence admits the truth of the State's evidence and all reasonable inferences therefrom. *State v. Salinas*, 119 Wn.2d 192, 201, 829 P.2d 1068 (1992). A person is guilty of computer trespass in the First Degree when he or she intentionally gains access to a computer system or electronic database of another and the access was made with the intent to commit another crime. RCW 9A.52.110. A person is guilty of intercepting, recording or divulging a private communication when he or she intercepts or records private communications transmitted by telephone or other device between two or more individuals by any device designed to record and/or transmit said communications. RCW 9.73.030.

The evidence at trial showed Novick put a program on Ms. Maunu's phone without her permission and then accessed the program on multiple different occasions and caused conversations that Ms. Maunu had with other people, private communications in the privacy of her home, her

friend's home, her back yard, etc., to be recorded. These recordings were done without her knowledge, without her permission. When all the evidence is viewed in the light most favorable to the State, it is clear there is sufficient evidence that a crime was committed.

Novick argues the evidence is insufficient, yet he argues the facts from the defendant's testimony. The jury clearly rejected the defendant's version of events; the jury is who decides credibility of witnesses. Furthermore, in a sufficiency of the evidence claim, the evidence the State introduced is presumed to be true; it doesn't matter if Novick thinks the evidence is "flimsy." In this the Court presumes the truth of the State's evidence and takes all reasonable inferences to determine if the jury could have found the elements of the offenses beyond a reasonable doubt. The evidence clearly established that Novick is guilty beyond a reasonable doubt of computer trespass and intercepting, recording or divulging a private communication on eight separate occasions. Novick's claim of insufficiency of the evidence fails.

II. Double Jeopardy does not bar multiple convictions for computer trespass and intercepting, recording or divulging a private communication.

Novick argues that he committed only one count of computer trespass and one count of interception of conversations because it was a

continuing course of conduct. Novick's claim is nonsensical and without any merit. Novick's claim fails.

The Double Jeopardy clause of the Fifth Amendment to the United States Constitution, and article I, section 9 of the Washington State Constitution prohibits the imposition of multiple punishments for the same offense. *State v. Adel*, 136 Wn.2d 629, 632, 965 P.2d 1072 (1998) (citing *State v. Gocken*, 127 Wn.2d 95, 100, 896 P.2d 1267 (1995) and *State v. Calle*, 125 Wn.2d 769, 772, 888 P.2d 155 (1995)). When a defendant is convicted of violating a single statute multiple times, the inquiry is "what 'unit of prosecution' has the Legislature intended as the punishable act under the specific criminal statute." *State v. Tili*, 139 Wn.2d 107, 113, 985 P.2d 365 (1999) (quoting *Adel*, 136 Wn.2d at 634 (citing *Bell v. United States*, 349 U.S. 81, 83, 75 S. Ct. 620, 99 L. Ed. 905 (1955) and *State v. Mason*, 31 Wn.App. 680, 685-87, 644 P.2d 710 (1982), *superseded on other grounds as stated in State v. Elliott*, 114 Wn.2d 6, 16, 785 P.2d 440 (1990)). If the Legislature has defined the scope of a criminal act, then double jeopardy provisions come into play and prevent a defendant from being convicted more than once for just one unit of the crime. *Adel*, 136 Wn.2d at 634.

In a unit of prosecution analysis, the first step is to analyze the criminal statute. *Adel*, 136 Wn.2d at 635. A person is guilty of computer

trespass in the first degree when he or she intentionally gains access to a computer system or electronic database of another and the access was made with the intent to commit another crime. RCW 9A.52.110. A person is guilty of intercepting, recording or divulging a private communication when he or she intercepts or records private communications transmitted by telephone or other device between two or more individuals by any device designed to record and/or transmit said communications. RCW 9.73.030. From the clear language of the computer trespass statute, a person commits the crime each time he gains access to another computer. This should be seen as similar to the criminal trespass statute which prohibits a person from knowingly entering or remaining in a building. No one would suggest the criminal trespass statute allows a person to trespass multiple times over the course of three months as long as it was the same building. This is what Novick attempts to argue here with regarding to computer trespass.

Novick argues he can only be guilty of one count of computer trespass and interception because it was the same victim and the same computer and thus a continuing course of conduct. However, under Novick's argument, it's feasible a person could illegally access the same person's computer over and over and over again, even after being arrested, tried and convicted for computer trespass, without committing a second

offense. It's possible under Novick's argument that a person could be charged and convicted of computer trespass, serve a sentence, be released into the community and illegally access the same computer without consent again, and not be guilty of another crime because the computer remained the same. This is a nonsensical approach and clearly not what the legislature intended. This is an absurd result and certainly not what the legislature intended, and does not stem from a logical, plain reading of the statutes involved.

The State has found no cases directly on point to answer this question, nor does Novick cite to any. However, reviewing cases that discuss the unit of prosecution issue as it applies to other charges is helpful in determining what the unit of prosecution is for computer trespass and interception. In *State v. Chouap*, 170 Wn. App. 114, 285 P.3d 138 (2012), the court determined what constituted separate units of Attempting to Elude a Pursuing Police Vehicle. There, the Court found that the defendant was properly convicted of two counts of Attempting to Elude as the defendant was twice pursued by police, the second pursuit separated from time by the first, and the defendant returned to lawful driving in between times. *Chouap*, 170 Wn.App. at 125.

In *State v. Hall*, 168 Wn.2d 726, 230 P.3d 1048 (2010), the Supreme Court goes through a lengthy analysis of what constitutes a unit

of prosecution. In *Hall*, the Court found that for witness tampering, the unit of prosecution was attempting to induce a witness to testify, and that could take a minute, 30 minutes or days. *Hall*, 168 Wn.2d at 731.

However, the Court went on to discuss possible scenarios when multiple units of prosecution may exist. For example, “if he had been stopped by the State briefly and found a way to resume his witness tampering campaign” or his “attempts to induce [were] interrupted by a substantial period of time, employ[ed] new and different methods of communications, [or] involve[d] intermediaries,” multiple units of prosecution may exist. *Id.* at 737-38.

This is the type of situation involved in Novick’s case. Novick stopped after his initial conduct; he had time to think about his actions, and deliberate and re-engage in his behavior, over and over again, on different days spanning months. As the Court in *Tili* adopted, “one should not be allowed to take advantage of the fact that he has already committed one sexual assault on the victim and thereby be permitted to commit further assaults on the same person with no risk of further punishment for each assault committed.” *State v. Tili*, 139 Wn.2d 107, 117, 985 P.2d 365 (1999) (quoting *Harrell v. State*, 88 Wis. 2d 546, 277 N.W.2d 462, 469 (1979)). Here, if Novick’s argument is accepted, then Novick could serve his sentence for Computer Trespass, find the victim after being released

from prison, and again trespass against her cellphone, as long as it is the same cell phone she had before. However, if Ms. Maunu had changed cell phones he would be guilty of multiple crimes as it was a different cell phone. This is an absurd reading of the statute. This is clearly not how the Legislature intended the crime to be punished. Under the statute, it is clear that each conversation and each trespass is punished separately, and is its own unit of prosecution. Novick was properly convicted of eight counts of Computer Trespass in the First Degree and eight counts of Interception as he did eight very distinct, very separate acts of accessing the cell phone by going to a website and commanding the phone to record and recorded eight different conversations involving Ms. Maunu. Novick was properly convicted and punished for each crime he committed. Novick's eight convictions of Computer Trespass in the First Degree and eight counts of Interception should be affirmed.

CONCLUSION

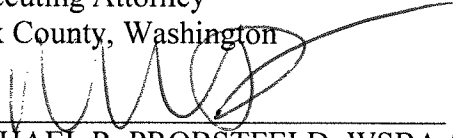
Novick was convicted upon sufficient evidence and double jeopardy does not bar multiple convictions for his distinct crimes. The trial court should be affirmed in all respects.

DATED this 2nd day of February 2016.

Respectfully submitted:

ANTHONY F. GOLIK
Prosecuting Attorney
Clark County, Washington

By:



RACHAEL R. PROBSTFELD, WSBA #37878
Senior Deputy Prosecuting Attorney
Office ID No. 91127

CLARK COUNTY PROSECUTOR

February 02, 2016 - 12:24 PM

Transmittal Letter

Document Uploaded: 3-476886-Respondent's Brief.pdf

Case Name: State v. David 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: Respondent's

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:

No Comments were entered.

Sender Name: Pamela M Bradshaw - Email: Pamela.Bradshaw@clark.wa.gov

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

David@DavidZuckermanLaw.com

brian@brianwalkerlawfirm.com