

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 URL¹ 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 trespass² and eight counts of recording private communications³ 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.

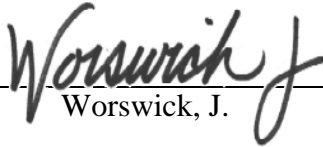
State v. Kinneman, 120 Wn. App. 327, 84 P.3d 882 (2003), addressed a similar issue. There, Kinneman made 67 unauthorized withdrawals from an individual's trust account. *Kinneman*, 120 Wn. App. at 327. The State charged Kinneman separately for each withdrawal resulting in 28 counts of first degree theft 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.

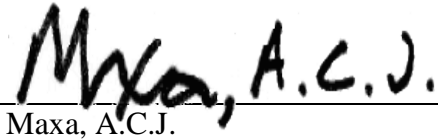
We hold that Novick's eight convictions for first degree computer trespass and eight convictions for recording private conversations do not violate double jeopardy principles because he was not charged multiple times for the same offense. Each count was based on evidence of eight distinct times that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

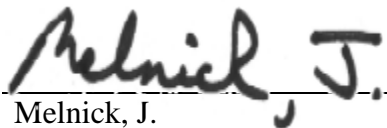
CONCLUSION

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.

We concur:


Maxa, A.C.J.


Melnick, J.