

STATE O F MICHIGAN
COURT O F APPEALS

PEOPLE OF THE STATE OF MICHIGAN,

Plaintiff-Appellee,

v

LEON JERMANE WALKER,

Defendant-Appellant.

UNPUBLISHED
December 27, 2011

No. 304593
Oakland Circuit Court
LC No. 2010-230991-FH

PEOPLE OF THE STATE OF MICHIGAN,

Plaintiff-Appellee,

v

LEON JERMANE WALKER,

Defendant-Appellant.

No. 304702
Oakland Circuit Court
LC No. 2011-236898-FH

Before: O'CONNELL, P.J., and MURRAY and

DONOFRIO, JJ. PER CURIAM.

These cases involve two consolidated, interlocutory appeals from separate lower court files involving the same defendant. In Docket No. 304593, defendant appeals by leave granted¹ the circuit court's order denying his motion to stay circuit court proceedings. In Docket No. 304702, defendant appeals by leave granted² the circuit court's order denying his motion to quash the information and dismiss the case. We affirm in both cases.

I. FACTS AND PROCEEDINGS

In Docket No. 304593, the charge against defendant arises from his alleged unauthorized access to the password-protected email account of his estranged wife, Clara Elizabeth Walker, from July 2009 through August 2009. At the preliminary exam, Clara testified that she filed for divorce from defendant on June 5, 2009, and that defendant had been served with the divorce papers by July 2009. Clara and defendant continued to live in the same home through August 2009. During this time period,

Clara had a personal email account through Gmail and another email account through Yahoo. Clara never shared her passwords for these email accounts with defendant, nor did she ever give defendant permission to access those accounts.³ During this same time period, Clara was regularly communicating by email on her Gmail account with a friend named Angela Vrtis.

On August 4, 2009, Clara was served with an emergency custody motion filed by her first ex-husband, Bryan Rudd, with whom she shared a child. Attached to the motion were emails between Clara and Vrtis, taken from Clara's Gmail account. The emails revealed that Clara was having an affair with her second ex-husband, Michael Johnston, during her marriage to defendant, her third husband. Clara never gave anyone permission to access those emails or to attach them to the motion. According to Clara, defendant-who works for the Oakland County Information Technology Department maintaining and setting up computers-stated at a Friend of the Court evidentiary hearing "that yes, he got my e-mails and he would do it again if he had to."

Clara testified that she used a computer that defendant bought her for her use. Defendant set up the computer for her, but Clara set up the Gmail and Yahoo accounts herself. Although Clara had previously written passwords in an address book, she has not used the address book for passwords in many years and never provided defendant with those passwords. Clara testified that she had never written a pass code for defendant on a sticky note, and that she allowed defendant to use her computer only when it needed a repair. Defendant had two computers of his own at home, and Clara did not know the passwords for defendant's computers.

Rudd testified that Clara is his ex-wife, and that in July 2009 defendant came to Rudd's home and gave him emails written by Clara to Vrtis. Defendant told Rudd that he had obtained the emails from his home computer. The emails caused Rudd to be concerned for the health, safety, and welfare of his child.

Sergeant Joe Brian, the officer-in-charge, spoke to defendant on December 15, 2009, at which time defendant "admitted to looking up and pulling off e-mails of his wife's account." Defendant told Brian that he had guessed the password for Clara's Gmail account, and that he accessed the emails from his computer at his home. Brian then asked defendant if Clara had "changed her password, he acknowledged that she did and I said did you guess those passwords as well and something to the effect of um, sort of, there's more to it then [sic] that. And then he didn't want to answer anymore [sic] questions."

At the conclusion of a preliminary examination, defendant was bound over for trial. The district court found that Clara did not share her computer password with defendant, and defendant did not ask Clara for her information. The district court analogized the Gmail account to a locked vault containing secured information. "Gmail allows a user to create a password which creates an expectation of privacy and creates security for the user. It's the user that decides who can have access to the information inside of the computer account, which in this case is like a vault." Although

defendant could touch the computer hardware, "he can't get access to what's inside the computer unless he has permission. The Court finds he didn't in this case. I'm satisfied the Prosecutor's met their burden of proof on a probable cause standard that during the time frame within this Court's jurisdiction Mr. Walker without valid authorization did acquire information involving the Google Gmail computer system and he did it without the permission of the password holder and the account holder contrary to MCL 752.795."

Following the bind over, defendant moved in the circuit court to quash the complaint. Defendant argued that the statute under which he was charged, MCL 752.795, prohibits the unauthorized access of computers, computer programs, computers systems, and computer networks, and that an email account does not fall under any of those categories as they are defined in MCL 752.792. In response, the prosecutor argued that the preliminary examination testimony showed that defendant violated MCL 752.795 when he accessed Clara's emails in her Gmail account, without her consent, and then shared the emails with Rudd. The prosecutor argued that if the circuit court required expert testimony regarding whether an email account constitutes a computer, computer network, computer program, or computer system, it should remand the case to the district court to hear expert testimony on the issue. The circuit court remanded the case to the district court "for expert testimony as to whether or not e-mail qualifies under the provisions of the statute."

On remand to the district court, Detective Carol Liposky of the Oakland County Sheriff's Department computer crimes unit testified as an expert on computer crimes and computer forensic issues. Liposky explained that Gmail is an email client in which a person signs up for an account using an email address and a password, allowing access to the email account. A user's messages are stored on the Gmail server, which is "a set of computers that have several [sic] hard disc space for multiple storages [sic] units." A server is a computer, and without a password, a person could not access emails. "When you go to log in, it will say what your e-mail address is and then ask for your password. It then ships it via the Internet, via the lines, makes several hops to get to the Gmail server." "A hop is all of the destinations it took to get from, if you're at home, from your home computer to the server client." Because Google and Gmail "are located in California, it's going to take all the computers that network through the Internet to hop from space to space to get to that Gmail server to authenticate, this is your e-mail address, this is your password. It then accepts it or denies it and then ships it back via the hops again." New emails are stored on the server. Liposky further explained that Gmail is a computer program, which she defined as "a sequential set of instructions that are put together to perform a certain task." "Gmail is written by programmers to perform a certain task, mainly be an e-mail client for your use to send out e-mails, accept incoming e-mails, deletion. All that's programmed in there to perform that specific task."

On cross-examination, Liposky further explained that Gmail “is a computer program which you access via the Internet to access your e-mail account. So it’s programming written in Java Script to perform its duties, perform a certain task. It uses the Internet as a way of getting to and from.” Liposky defined a computer as “an electronic device to access data and perform logical mathematical functions. Those servers are performing those functions; therefore, it is a computer system.” When asked whether an individual Gmail account is a computer network, Liposky answered, “It is on servers, which are computers, which are interconnected to other — because I’m not sure how many servers they need. So it could be connected to other servers. So I can’t answer that question.”

When asked by the district court which part of the statute gave her reason to believe that email meets the definitions contained in the statute, Liposky stated, “I would say computer program, computer system, computer network, computer, all three [sic], as paragraphed here, three, four, five, and six, because it’s totality [sic] of what’s going on. She’s accessing it using a computer, she’s using the Internet, which is a computer network, and a program such as Gmail, that it [sic] was created specifically for e-mail.”

At the conclusion of the hearing, the district court again bound defendant over as charged. The court accepted Liposky’s expert testimony that Gmail is a computer system and, although the statute does not refer to email, the district court analogized the case to a felonious assault where a gun was used but an item such as a bullet or gun powder that is not specifically named in the statute harmed the victim:

So it doesn’t trouble the Court, is my point, that e-mail as a word or electronic mail as a phrase is not specifically mentioned in the statute. Keyboard is not mentioned. Hard drive is not mentioned. Screen is not mentioned. And I think that we’re going way beyond what we need to do if we want to consider the spirit of the law and what it was intended to prevent and protect.

And so I wanted to make it clear. It’s not troubling to the Court that that word or phrase is not here. It’s encompassed in a computer program or system or network, just like in a weapon there could be gun powder or a bullet or a holster or anything else that can be used in a crime.

So whether it is part of a system, network, or program or whether it is the system or network or program, I am finding that the prosecutor has met their burden of proof on a probable cause standard to have the matter bound over again to the Oakland County Circuit Court.

When the case returned to the circuit court, defendant submitted to the circuit court a renewed motion to quash. At a hearing held on December 8, 2010, the circuit court concluded that the matter should proceed to trial: “I believe the People have met their burden of probable cause and that [Liposky’s] testimony was sufficient for bind over and is sufficient for this court to determine e-mails fall within the meaning of the statute. So I am denying your motion to quash.” The circuit court did not, however,

enter an order denying the motion to quash following the December 8, 2010, hearing.

On January 19, 2011, the prosecutor moved for a hearing to admit similar acts evidence. The prosecutor stated that in April 2010, defendant used his position as an employee of the Oakland County IT unit to gain access to the Court and Law Enforcement Management Information System (CLEMIS) in the IT building. At a hearing held on March 2, 2011, the circuit court concluded “that there is enough here for this court to hold an evidentiary hearing to determine whether or not the court will grant the People’s request to have similar acts under 404(b) admitted.” On March 23, 2011, however, defense counsel stated informed the court that, “I talked it over with my client, and we have withdrawn our objection to that so-called prior act evidence, so if and when the case is tried, if the government seeks to introduce that evidence, we’re not going to object to it so, therefore, we didn’t need an evidentiary hearing.” The circuit court therefore granted the prosecutor’s request “to place into the court file the statements — the memos that you have” regarding the other acts evidence. The prosecutor then filed memos prepared by CLEMIS employees regarding the similar acts.

On May 31, 2011, the circuit court entered an order denying defendant’s motion for a stay of circuit court proceedings, in accordance with its May 4, 2011, oral ruling from the bench. On June 15, 2011, defendant filed an application for leave to appeal the circuit court’s May 31, 2011, order denying defendant’s motion to stay the circuit court proceedings. In addition, defendant moved in this Court to stay the circuit court proceedings and for immediate consideration of the motion to stay. This Court issued an order granting the motion for immediate consideration and staying further proceedings pending resolution of the appeal or further order of this Court. This Court’s order further provided:

In lieu of granting leave to appeal, pursuant to MCR 7.205(D)(2) and MCR 7.216(A)(3), (5) and (9), the Court orders the case REMANDED to the circuit court, which is directed to issue a written opinion and order addressing defendant’s motion to quash and whether defendant’s alleged conduct falls within the scope, intent, and purpose behind MCL 752.795. This Court concludes that serious questions exist as to whether this felony criminal statute was intended to be applied to domestic relations cases of the sort presented here. [*People v Walker*, unpublished order of the Court of Appeals, entered June 20, 2011 (Docket No. 304593).]

This Court’s order directed the parties to file briefs in this Court following the issuance of the circuit court’s written opinion and order. *People v Walker*, unpublished order of the Court of Appeals, entered June 20, 2011 (Docket No. 304593).

On remand, the circuit court issued a thorough written opinion and order denying defendant’s motion to quash. The court began by noting that “this is *not* a domestic relations matter. Defendant is charged with one count of Unauthorized Access of a Computer in violation of MCL 752.795, a *criminal statute*.” After summarizing

the factual background and procedural history of the case, the circuit court articulated its reasons for denying defendant's motion to quash. Although the word "email" does not appear in the statute, the circuit court found it inconceivable that an email account, belonging to an individual, corporate entity or otherwise, is immune from the protections of the statute. If Defendant's position were to be accepted, anyone could impermissibly access the email account of another, such as Google or Yahoo simply because these email accounts are Internet based, can be accessed remotely and are not terminal specific. These facts alone should not shield a person from liability by accessing the account of another. Otherwise, why would email accounts be password protected and have detailed privacy policies? Further, as testified by Detective Liposky, email is considered a 'computer program, computer system, computer network, computer . . . [s]he's accessing it using a computer, she's using the Internet, which is a computer network, and a program such as Gmail, that it [sic] was created specifically for email.' As indicated by Detective Liposky, the Internet is itself, a 'computer network' as contemplated by the statute and without the Internet, one would be unable to access his or her email. Query, what is email, if not a computer network, system or program? Accordingly, the Court believes email falls within the framework of MCL 752.792. Based on the testimony presented at both exams, the Courts finds there was a sufficient record to support a probable cause finding and therefore no abuse of discretion.

Just as Defendant so emphatically emphasizes that the word email does not appear within the statute, the Court would also like to emphasize that the statute contains no spousal exception. This matter has been referred to as the 'spousal email case' or a 'domestic relations case' and the fact that these parties were married at the time of the alleged offense has generated considerable outrage that 1) Defendant has been charged; and 2) this Court has not dismissed the case. It is unclear to the Court where the spousal rationale that has been used in support of dismissal has any support? [sic] Defense counsel has repeatedly advised the Court that the Legislature will imminently take remedial and retroactive measures to amend the statute so as to enact some type of spousal exception. However, unless and until such legislation occurs, this Court is left with the statute as written. This Court does not legislate from the bench; rather it interprets the law as written. 'Whether conduct falls within the scope of a penal statute is a question of statutory interpretation.' *People v Flick*, 487 Mich 1, 8; 780 NW2d 295 (2010). The Court has articulated its reasons above for finding that email falls within the statutory framework of MCL 752.795. The Court will not create a 'spousal exception' where one does not exist. The plain language of the statute reveals no support for such an exception.

The circuit court further noted that a spousal exception would be akin to a person somehow bypassing the log-on feature requiring entry of a username and password simply by being the spouse of an account holder. Lastly, court commented upon the limited role it played in determining whether the cases should proceed to trial:

as a member of the Judiciary, it is not the role of this Court to usurp the

authority of the Oakland County Prosecutor by second-guessing her decision to charge this case. Rather, as a judge, the Court presides over and tries cases. It has been repeatedly been [sic] suggested that Defendant has been 'singled out' and that no other individual in a spousal situation such as Defendant has been charged for similar conduct. Again, this court is not privy to, nor does it concern itself with what factors into the Prosecutor's charging decisions. Further, it is of no concern to the Court whether no other spouses in Defendant's situation have been charged for similar acts; what the Court does know is that it is following the law, as written, and trying to expeditiously resolve this case.

Following the issuance of the circuit court's written opinion and order, the parties filed briefs in this Court. This Court then granted defendant's application for leave to appeal, "limited to the issues of whether defendant's alleged conduct falls under MCL 752.795 and whether the circuit court erred in denying defendant's motion to quash the charge." This Court continued the stay of proceedings previously granted and ordered the appeal expedited. *People v Walker*, unpublished order of the Court of Appeals, entered September 6, 2011 (Docket No. 304593).

II. ANALYSIS

In Docket No. 304593, defendant argues that the circuit court erred in denying his motion to quash the charge alleging unauthorized access of a computer, MCL 752.795. This Court reviews for an abuse of discretion a district court's decision to bind over a defendant. *People v Hudson*, 241 Mich App 268, 276; 615 NW2d 784 (2000). "An abuse of discretion occurs when the court chooses an outcome that falls outside the range of reasonable and principled outcomes." *People v Unger*, 278 Mich App 210, 217; 749 NW2d 272 (2008). "A circuit court's decision with respect to a motion to quash a bindover order is not entitled to deference because this Court applies the same standard of review to this issue as the circuit court. This Court therefore essentially sits in the same position as the circuit court when determining whether the district court abused its discretion." *Hudson*, 241 Mich App at 276. "The decision whether alleged conduct falls within the statutory scope of a criminal law involves a question of law, which this Court reviews de novo." *People v Noble*, 238 Mich App 647, 658; 608 NW2d 123 (1999).

In *People v Henderson*, 282 Mich App 307, 312; 765 NW2d 619 (2009), this Court explained:

The primary function of the preliminary examination is to determine whether a crime has been committed and, if so, whether there is probable cause to believe that the defendant committed it. Probable cause that the defendant has committed a crime is established by evidence sufficient to cause a person of ordinary prudence and caution to conscientiously entertain a reasonable belief of the defendant's guilt. To establish that a crime has been committed, a prosecutor need not prove each element beyond a reasonable doubt, but must present some evidence of each element. Circumstantial evidence and reasonable

inferences from the evidence can be sufficient. If the evidence conflicts or raises a reasonable doubt, the defendant should be bound over for trial, where the questions can be resolved by the trier of fact. [Citations omitted.]

In *People v Phillips*, 469 Mich 390, 395; 666 NW2d 657 (2003), the Michigan Supreme Court set forth the following principles of statutory interpretation:

When construing a statute, our primary goal is to ascertain and give effect to the intent of the Legislature. To do so, we begin by examining the language of the statute. If the statute's language is clear and unambiguous, we assume that the Legislature intended its plain meaning and the statute is enforced as written. Stated differently, a court may read nothing into an unambiguous statute that is not within the manifest intent of the Legislature as derived from the words of the statute itself. Only where the statutory language is ambiguous may a court properly go beyond the words of the statute to ascertain legislative intent. [Citations, quotations, and footnote omitted.]

To begin, we emphasize, as did the circuit court, that whether charges should be brought against this defendant constitutionally falls within the exclusive discretion of the prosecuting attorney. "The county prosecutor is a constitutional officer with discretion to decide whether to initiate criminal charges." *People v Herrick*, 216 Mich App 594, 598; 550 NW2d 541 (1996). "The principle of separation of powers restricts judicial interference with a prosecutor's exercise of executive discretion." *Id.* Consequently, whether it is the best policy to prosecute this defendant under these circumstances is not our duty to decide. Rather, we only determine whether the district court abused its discretion in ruling that the prosecutor brought forward sufficient facts to establish probable cause to believe that defendant committed the crimes charged.

Here, defendant was charged with unauthorized access of a computer, MCL 752.795. That statute provides:

A person shall not intentionally and without authorization or by exceeding valid authorization do any of the following:

(a) Access or cause access to be made to a computer program, computer, computer system, or computer network to acquire, alter, damage, delete, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network.

(b) Insert or attach or knowingly create the opportunity for an unknowing and unwanted insertion or attachment of a set of instructions or a computer program into a computer program, computer, computer system, or computer network, that is intended to acquire, alter, damage, delete, disrupt, or destroy property or otherwise use the services of a computer program, computer, computer system, or computer network. This subdivision does not prohibit conduct protected under section 5 of article I

of the state constitution of 1963 or under the first amendment of the constitution of the United States. [MCL 752.795.]

Like many cases, the statutorily provided definitions are important to resolving this case. MCL 752.792(1) defines “access” as “to instruct, communicate with, store data in, retrieve or intercept data from, or otherwise use the resources of a computer program, computer, computer system, or computer network.” A “computer” is defined as “any connected, directly interoperable or interactive device, equipment, or facility that uses a computer program or other instructions to perform specific operations including logical, arithmetic, or memory functions with or on computer data or a computer program and that can store, retrieve, alter, or communicate the results of the operations to a person, computer program, computer, computer system, or computer network.” MCL 752.792(3). “‘Computer network’ means the interconnection of hardware or wireless communication lines with a computer through remote terminals, or a complex consisting of 2 or more interconnected computers.” MCL 752.792(4). MCL 752.792(5) defines a “computer program” as “a series of internal or external instructions communicated in a form acceptable to a computer that directs the functioning of a computer, computer system, or computer network in a manner designed to provide or produce products or results from the computer, computer system, or computer network.” A “‘computer system’ means a set of related, connected or unconnected, computer equipment, devices, software, or hardware.” MCL 752.792(6). “‘Property’ includes, but is not limited to, intellectual property, computer data, instructions or programs in either machine or human readable form, financial instruments or information, medical information, restricted personal information, or any other tangible or intangible item of value.” MCL 752.793(1). “‘Services’ includes, but is not limited to, computer time, data processing, storage functions, computer memory, or the unauthorized use of a computer program, computer, computer system, or computer network, or communication facilities connected or related to a computer, computer system, or computer network.” MCL 752.793(2).

Although there are no cases setting forth the elements of unauthorized access of a computer, the elements can be discerned from the unambiguous language of MCL 752.795. The language at issue states that “[a] person shall not intentionally and without authorization or by exceeding valid authorization . . . [a]ccess or cause access to be made to a computer program, computer, computer system, or computer network to acquire, alter, damage, delete, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network.” MCL 752.795(a). Accordingly, the plain and ordinary meaning of this statutory text reflects that the following elements must be established: the defendant must have (1) intentionally and (2) without authorization or by exceeding valid authorization (3) accessed or caused access to be made to a computer program, computer, computer system, or computer network (4) to acquire, alter, damage, delete, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network. Because the statutory language clearly sets forth these elements, it is not proper to “go beyond the words of the statute to ascertain legislative intent.” *Phillips*, 469 Mich at 395 (quotations and citation omitted).⁴

Sufficient evidence was presented regarding each element to support the district court's decision to bind defendant over for trial. First, the evidence supports a reasonable inference that defendant acted intentionally. "A statute that requires a prosecutor to prove that the defendant intended to perform the criminal act creates a general intent crime. A statute that requires proof that the defendant had a particular criminal intent beyond the act done creates a specific intent crime." *People v Herndon*, 246 Mich App 371, 385; 633 NW2d 376 (2001) (footnotes and quotations omitted). There is nothing in the language of MCL 752.795 to suggest that the prosecutor must prove a particular intent beyond the intent to perform the criminal act. Thus, the statute creates a general intent crime.

A defendant's intent can be inferred from circumstantial evidence, including the defendant's words or "the act, means, or the manner employed to commit the offense." *People v Hawkins*, 245 Mich App 439, 458; 628 NW2d 105 (2001). Here, defendant admitted to the police that he accessed his estranged wife's Gmail account after guessing her password. Defendant then gave copies of her emails to a third party. Thus, a reasonable inference can be drawn that defendant acted intentionally when he accessed his wife's Gmail account, used the account to view her email messages, and printed the messages to distribute to a third party.

Second, there was evidence that defendant acted without authorization when he accessed his estranged wife's Gmail account. Defendant's wife testified that her Gmail account was a personal account and that she never shared her passwords for the account with defendant or granted him permission to access the account. Further, she allowed defendant to use her computer only when it needed a repair. Defendant admitted to the police that he accessed his wife's Gmail account by guessing her password. These facts support a reasonable inference that defendant lacked authorization for his access of his wife's Gmail account.

Next, the evidence at the preliminary examinations established that defendant accessed or caused access to be made to a computer program, computer, computer system, or computer network. Detective Carol Liposky, testifying as an expert on computer crimes and computer forensic issues, explained that a user's messages are stored on the Gmail server. A server is a computer. The emails cannot be accessed without a password. After a user signs in with a valid password, email messages are retrieved from the Gmail server through the Internet. The Internet is a computer network. Further, Gmail is a computer program because it is written by programmers to perform certain tasks, i.e., to function as an email client by which users can send emails, accept incoming emails, and delete emails. The Gmail servers act as a computer system by performing the required functions. Thus, Liposky opined that by accessing Gmail, a person uses a computer program, a computer system, a computer network, and a computer. "She's accessing it using a computer, she's using the Internet, which is a computer network, and a program such as Gmail, that it [sic] was created specifically for e-mail." Thus, the evidence supports a conclusion that by guessing his wife's password and then using her Gmail account, defendant accessed or

caused access to be made to a computer program, computer, computer system, or computer network.

Finally, the prosecutor presented evidence that defendant acquired, altered, damaged, deleted, or destroyed property or otherwise used the service of a computer program, computer, computer system, or computer network. Defendant used the services of Gmail when he gained access to his estranged wife's account, viewed her emails, and printed them to distribute to a third party. Further, by viewing, printing, and distributing the emails, defendant acquired his wife's property, i.e., her password-protected emails containing restricted personal information or other tangible or intangible items of value. MCL 752.793(1).

Accordingly, we conclude that the prosecutor presented sufficient evidence of each element of unauthorized access of a computer, MCL 752.795, to support the district court's decision to bind defendant over for trial.

In Docket No. 304702, defendant first argues that the circuit court erred in denying his motion to quash a separate charge alleging unauthorized access of a computer, MCL 752.795. We reject defendant's argument, however, because sufficient evidence was presented regarding each element to support the district court's decision to bind defendant over for trial. First, the evidence supports a reasonable inference that defendant acted intentionally. In this case, defendant, an employee of the Oakland County Information Technology (IT) department, was made aware that, in light of the separate charge against him in the email case, he was no longer allowed to access any law enforcement or court computer systems, including the Court and Law Enforcement Management Information System (CLEMIS). Despite this restriction, defendant went to the office of Leanne Marie Robinson, a CLEMIS employee, and remained silent until her boss left the area. He then closed Robinson's door and asked if it was possible to search for words in NET RMS, the police records program. Robinson introduced defendant to Laura Harper, the administrator for NET RMS, who showed defendant how to navigate through NET RMS. When asked the reason for his inquiries, defendant indicated that he was assisting Angela Susalla, a Sheriff's Department employee, and did not reveal that he was there for personal reasons or that he was restricted from having any contact with CLEMIS employees. Susalla testified that she did not give defendant permission to use her name or to say that he was assisting her.

In light of defendant's alleged conduct, including (1) his failure to reveal the personal nature of his business, (2) his failure to disclose the restriction barring him from contacting CLEMIS employees, and (3) his false representation that he was assisting Susalla, a reasonable inference could be drawn that defendant acted intentionally when he caused Harper to access CLEMIS. It could fairly be concluded from these facts that defendant was seeking to acquire, for his personal use, restricted information regarding how to navigate through the NET RMS system and conduct searches.

Second, there was evidence that defendant acted without authorization when he caused Harper to access CLEMIS. Defendant's supervisor, Kevin Bertram, testified

that in February 2010, defendant was made aware that he was no longer allowed to access any law enforcement or court computer systems, including CLEMIS. Defendant was not allowed to touch CLEMIS computers or talk to CLEMIS division employees. Robinson testified that CLEMIS employees cannot tell the general public how NET RMS works or demonstrate to them how it works. Defendant was suspended for five days for his actions in the CLEMIS matter. Thus, evidence was presented that defendant lacked authorization to cause access to CLEMIS to be made.

Next, the evidence supported a conclusion that defendant accessed or caused access to be made to a computer program, computer, computer system, or computer network. Bertram explained that NET RMS is a computer system that police agencies use to record incidents, including police [reports](#). NET RMS is part of CLEMIS. After Robinson introduced defendant to Harper, defendant stated that he was doing some work with Susalla, that she did not know how to do a word search in the narratives of the police reports, and that he wanted to know if there was a way to do that. Based on the statements of Robinson and defendant, Harper accessed CLEMIS. Harper indicated that defendant's statements caused her to access CLEMIS. Thus, sufficient evidence was presented that defendant caused access to a computer system to be made.

Finally, the prosecutor presented evidence that defendant acquired property or otherwise used the service of a computer program, computer, computer system, or computer network. After Harper accessed CLEMIS, she navigated through the system as defendant was sitting next to her. Defendant was thus learning how to navigate through NET RMS. Harper pulled up a document from the Macomb County Police Department, and defendant saw that as he was sitting next to her. Defendant was watching what Harper was doing, and she was explaining it to him. Robinson testified that CLEMIS employees cannot tell the general public how NET RMS works or demonstrate to them how it works. The police data in the system belongs to the police department, and CLEMIS employees do not give out the information without a proper request. Harper testified that she had a concern that defendant, given his position, could remotely access CLEMIS and obtain the information himself, after she had showed him how to perform searches. Bertram became aware that defendant had accessed another CLEMIS employee's computer after he was told not to do so, in contravention of the order that he may not access the computers of CLEMIS employees.

Thus, a reasonable inference could be drawn that defendant caused Harper to use NET RMS in his presence so that he could learn how to navigate through the system and to conduct narrative word or phrase searches. Defendant thereby acquired restricted information regarding the functioning of a secure computer system, information that a reasonable fact finder could determine constituted a tangible or intangible item of value. MCL 752.793(1). Thus, the prosecutor presented sufficient evidence to establish probable cause that defendant committed the crime of unauthorized access of a computer.

Defendant's final argument on appeal is that the circuit court erred in deciding to sever the email case and the CLEMIS case and in denying defendant's motion to

stay circuit court proceedings in the CLEMIS case pending the appeal in the email case.⁵ “To determine whether joinder is permissible, a trial court must first find the relevant facts and then must decide whether those facts constitute ‘related’ offenses for which joinder is appropriate.” *People v Williams*, 483 Mich 226, 231; 769 NW2d 605 (2009). Questions of law are reviewed de novo, and factual findings are reviewed for clear error. *Id.* Because the circuit court here did not make any findings of fact regarding joinder, this Court’s review is de novo.

Defendant has not established that the circuit court erred in declining to join the cases. Initially, defendant contends that the circuit court improperly severed the two cases. However, because the charges were filed separately and no order of joinder or consolidation was entered, the circuit court did not sever the cases. In addition, defendant did not file a formal motion requesting joinder, although the parties agreed on the record before this Court that the cases should be tried together. Consequently, we need not address whether the trial court should join those cases for trial on remand.

Affirmed in both cases.

/s/ Peter D. O’Connell
/s/ Christopher M.
Murray /s/ Pat M.
Donofrio

Footnotes

1 *People v Walker*, unpublished order of the Court of Appeals, entered September 6, 2011 (Docket No. 304593).

2 *People v Walker*, unpublished order of the Court of Appeals, entered June 22, 2011 (Docket No. 304702).

3 According to Clara, sharing information was not common in their marriage, as she and defendant did not share bank account numbers, never filed joint tax returns, and never discussed financial information or commingled their finances.

4 Contrary to defendant’s argument, nothing in the statutory text suggests that spouses, estranged spouses, or parties to a divorce proceeding are immune from prosecution under the act. Further, the mere possibility that MCL 752.795 may be amended in the future does not affect this Court’s interpretation of the existing statutory language.

5 Initially, we conclude that the stay issue is moot. Generally, a court does not decide moot issues because its principal duty is to decide actual cases and controversies. *People v Richmond*, 486 Mich 29, 34; 782 NW2d 187 (2010)

reh gtd in part on other grounds 486 Mich 1041 (2010). Here, the issue whether the circuit court should have stayed the CLEMIS case pending the appeal in the email case is an abstract question of law that does not rest on existing facts or rights. Following the circuit court's denial of defendant's motion to stay, this Court, on the same date, granted defendant's motion for stay pending appeal. People v Walker, unpublished order of the Court of Appeals, entered June 22, 2011 (Docket No. 304702). The cases were then consolidated for appeal. People v Walker, unpublished order of the Court of Appeals, entered September 14, 2011 (Docket Nos. 304593 and 304702). Accordingly, any decision regarding whether the circuit court erred in denying defendant's motion to stay the CLEMIS case pending the appeal in the email case would have no practical legal effect on the case, because this Court has already provided relief to defendant by granting his motion for stay and consolidating the cases on appeal.