UNC SCHOOL OF GOVERNMENT

ADMINISTRATION OF JUSTICE BULLETIN NO. 2021/01 | AUGUST 2021

Computer-Related Crime in North Carolina

Brittany L. Williams

CONTENTS

Cybercrime, also known as computer crime, is a broad term for criminal activity committed by using a computer to illegally access, transmit, or manipulate data. Such activity can include fraud, child pornography, cyberbullying, stalking, intellectual-property theft, identity theft, violations of privacy, and other acts. Many of these crimes are committed by people who find weaknesses in computer systems and manipulate those systems to reach a desired end. Sadly, the law always seems to lag behind our ever-evolving technology and the new vulnerabilities that arise from it. Even still, there are some laws that are written broadly enough to encompass some of the most common forms of cybercrime.

North Carolina's computer-related-crime laws are in Article 60 of Chapter 14 of the General Statutes (hereinafter G.S.). These crimes include

- accessing computers;
- accessing government computers;
- damaging computers, computer programs, computer systems, computer networks, and resources;
- denial of computer services to an authorized user;

Brittany L. Williams is an assistant professor of criminal law at the School of Government. She works across all areas of criminal law and procedure but specializes in domestic violence and computer-related crimes.

- denial of government-computer services to an authorized user;
- extortion; and
- computer trespass.[1]

The statutes are filled with technical language and encompass several activities. This bulletin explores the acts prohibited by these statutes, how the statutes have been applied, and some common criminal scenarios that may fall within the purview of these statutes.

Definitions

Most of North Carolina's computer-related-crime statutes prohibit unauthorized access to computers, computer programs, computer systems, computer networks, and computer software. Each of these items is defined under G.S. 14-453.

Under the statute, a "computer" is an internally programmed, automatic device that performs data processing or telephone switching. This obviously includes personal computers, laptops, and desktops. Given the plain language of the statute, it likely includes cell phones, notebooks, and tablets, and it may include smart watches.

A "computer network" is the interconnection of communication systems with a computer through remote terminals, or a system consisting of two or more interconnected computers or telephone-switching equipment. This could include a mobile hotspot or a Wi-Fi router and any computers connected to such devices.

A "computer program" is an ordered set of coded instructions or statements that cause a computer to process data when the computer executes the instructions. Many people may interact with several computer programs a day. Some common examples include Microsoft Windows, Internet Explorer, Microsoft Office, Microsoft Outlook, Adobe Acrobat Reader, and various cellphone applications, including games, social-media apps, and communication apps.

"Computer services" is defined as computer time or services, including data processing, Internet services, electronic mail, electronic messaging, and any information or data stored in connection with any of these services. Computer services are often loaded automatically at startup and run in the background without user interaction (like the clock, for example). This also includes computer "cookies" and browsing history.

"Computer software" is a set of computer programs, procedures, and associated documentation concerned with the operation of a computer, computer system, or computer network. Antivirus software, audio programs, movie players, and word processors are some common examples. Mobile apps also fall under this category.

Finally, "computer system" is defined as at least one computer together with a set of related, connected, or unconnected peripheral devices. This is another term that encompasses desktops, laptops, and smartphones. Other components, like the monitor, keyboard, mouse, and speakers are considered peripheral devices that are part of the system.

1. Cyberbullying statutes G.S. 14-458.1 and -458.2 are also found in this article but are outside the scope of this bulletin, which focuses on the criminal use of computers themselves rather than its effects on a victim. Other crimes that involve computers (e.g., cyberstalking and solicitation of a child by computer) are found elsewhere in the General Statutes and are likewise outside the scope of this discussion.

Many of these terms overlap and can include some of the same items. The statutes typically list several overlapping terms individually (e.g., "any computer, computer program, computer system, computer network, or any part thereof")[2] so as not to inadvertently exclude any items as a medium for effectuating these crimes. Even so, it is probably safe to infer that the crimes encompass not only computers and other digital devices themselves but also any program or application that can be found on them and the systems that keep all these things functioning.

Accessing Computers and Accessing Government Computers

Access for Specified Purposes

Under G.S. 14-454(a), "[i]t is unlawful to willfully, directly or indirectly, access or cause to be accessed any computer, computer program, computer system, computer network, or any part thereof" in order to (1) devise or execute "any scheme or artifice to defraud" or (2) obtain property or services "by means of false or fraudulent pretenses, representations or promises."

G.S. 14-454.1 mirrors that statute but applies specifically to government computers. A government computer is "any computer, computer program, computer system, computer network, or any part thereof, that is owned, operated, or used by any State or local governmental entity."[3] Unlawful access of a computer in a police department, a public school, or the White House would fall under this statute. Unlawful access of a neighbor's computer would fall under G.S. 14-454.

Modes of Access

The plain language of these statutes allows for several possible ways for these crimes to occur. A defendant could directly access a computer, which might involve physically sitting down in front of the computer and using it without authorization. A defendant could also indirectly access a computer, which could be by means of remote-access software or through another person. The statute also provides for "causing to be accessed," which could encompass the latter situation.

In *State v. Bernard*, an employee at North Carolina A&T State University filed a complaint at the local police department alleging that someone accessed her university email account without her permission. She stated that someone accessed her email, constructed a bogus communication, and emailed the document to university administrators in an effort to rehire or compensate the defendant, who was a recently terminated employee. Detectives were able to trace the origin of the communication using the related IP address[4] and were led to the defendant. The defendant was indicted for accessing a government computer without authorization and felony accessing computers. The defendant directly accessed a state employee's email account at a university campus and sent an email that was intended to defraud. She was convicted, and the North Carolina Court of Appeals upheld this conviction.[5]

2. G.S. 14-454(a).

3. G.S. 14-453(7a).

4. An Internet-protocol (IP) address is a unique address that identifies a device on the Internet or a local network. IP addresses allow information to be sent between devices on a network; they contain location information and make devices accessible for communication. IP addresses provide a way of differentiating between different computers, routers, and websites.

5. 236 N.C. App. 134 (2014).

In *State v. Golder*, a defendant devised a scheme in which he paid an employee at the Wake County clerk's office to falsify bail-bond-forfeiture documents. Over the course of five years, the defendant sent text messages to the employee with lists of names and file numbers of cases in which bond forfeitures had been entered. After receiving a list from the defendant, the employee would enter a motion to set aside the bond forfeiture for each of the cases into the county's electronic records. After twenty days, the bond forfeiture would automatically be set aside, so the defendant's bail-bonding company would no longer be required to pay the bond. In exchange for entering the motions into the system, the defendant paid the employee $500 for each list of cases. The defendant was charged with accessing a government computer. Although the defendant had not entered the forfeitures into the computer system himself, he had caused the system to be accessed as prohibited by the statute. He was convicted, and both the court of appeals and the North Carolina Supreme Court upheld the conviction.[6]

Access for Other Purposes

Subsection (b) of the accessing-computers statute states that "any person who willfully and without authorization, directly or indirectly, accesses or causes to be accessed any computer, computer program, computer system, or computer network for any purpose other than those set forth in subsection (a) above, is guilty of a Class 1 misdemeanor." Unlike subsection (a), subsection (b) includes "without authorization" as an element.[7] "Authorization" is defined under G.S. 14-453(1a) as "having the consent or permission of the owner, or of the person licensed or authorized by the owner to grant consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission."

Because this subsection also requires access for any purpose other than fraud or obtaining property or services, this is likely to include acts like logging into someone's Facebook account without permission to post an inappropriate message or logging into someone's work computer without permission to delete files or emails.

The United States Supreme Court recently decided *Van Buren v. United States*, in which the Court clarified the scope of access covered by the federal Computer Fraud and Abuse Act.[8] The Act subjects to criminal liability anyone who "intentionally accesses a computer without authorization or exceeds authorized access."[9] The term "exceeds authorized access" is defined to mean "access[es] a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[10]

The Court held that the "exceeds authorized access" clause covers those who obtain information from particular areas in the computer to which their computer access does not extend, but it does not cover those who have improper motives for obtaining information that is otherwise available to them. Extending this holding to the North Carolina statute, accessing computers "without authorization" likely does not cover a scenario in which a police officer uses the police database to look up the address or criminal record of a love interest. The statute also

6. 374 N.C. 238 (2020).

7. G.S. 14-454(b).

8. ___ U.S. ___, 141 S. Ct. 1648 (2021). For the full case summary, see Brittany Williams, *Case Summaries—U.S. Supreme Court (June 1–3, 2021)*, N.C. Crim. L., UNC Sch. of Gov't Blog (June 7, 2021), https://nccriminallaw.sog.unc.edu/case-summaries-u-s-supreme-court-june-1-3-2021/.

9. 18 U.S.C. § 1030(a)(2).

10. 18 U.S.C. § 1030(e)(6).

likely does not cover more-common activities like checking personal email, checking personal social-media accounts, or booking travel for vacation on a work computer.[11]

Unlawful Access of Other Computers

The above cases deal with traditional computers like laptops and desktops. There is no case law that involves unauthorized access of other types of computers like phones and tablets, but accessing these types of devices likely falls within the statute's reach. It is not uncommon for people to gain entry into other people's cellphones for improper purposes, like sending themselves screenshots of messages, transferring money via mobile-payment applications like Cash App or Venmo, or sending themselves private pictures. The accessing-computers statutes likely encompass these intrusions. Although the statutes don't specify these acts, the acts could still satisfy each element of the appropriate statute.

With security features such as face recognition, fingerprint entry, and passcodes, it is reasonable to believe that a person who is using another person's phone has been given permission to do so unless the phone has been stolen and broken into. However, even with that permission, a person can act without authorization by exceeding the scope of that permission. Unless the owner gives permission for the user to perform the specific act at issue on the owner's computer (sending money or pictures, for example), that act may be deemed to have occurred without authorization.

Recall that subsection (a) does not require the computer to be accessed without authorization, and instead requires only willful access. *Willful* generally means performed intentionally and without an honest belief that there is an excuse or justification.[12] The access must have been for the additional purpose of committing fraud or of obtaining property or services. Sending oneself money from another person's mobile-banking app without that person's permission or knowledge can certainly be considered fraudulent. Screenshots of messages and private pictures can be considered property, as the statutory definition of *property* includes electronically processed or produced data.

Accessing Educational Materials

G.S. 14-454.1 includes an additional provision stating that "[a]ny person who willfully and without authorization, directly or indirectly, accesses or causes to be accessed any educational testing material or academic or vocational testing scores or grades in a government computer is guilty of a Class 1 misdemeanor."[13] There is currently no case law on this provision. This could include scenarios like a student using a teacher's computer to change his final grade or gain early access to test questions.

11. For more on this issue, see Brittany Williams, *"Authorization" in the Context of Computer Crimes*, N.C. Crim. L., UNC Sch. of Gov't. Blog (June 1, 2021), https://nccriminallaw.sog.unc.edu/authorization-in-the-context-of-computer-crimes/.

12. State v. Ramos, 193 N.C. App. 629, 636 (2008).

13. G.S. 14-454.1(c).

Damaging Computers

Under G.S. 14-455(a), "[i]t is unlawful to willfully and without authorization alter, damage, or destroy a computer, computer program, computer system, computer network, or any part thereof." If "the damage caused by the alteration, damage, or destruction is more than one thousand dollars ($1,000)," the offense is a Class G felony. Willful and unauthorized alteration, damage, or destruction of a government computer is a Class F felony. Any other violation involving damage to a computer is a Class 1 misdemeanor.

Damage to a computer does not have to render a computer inoperable to be charged under this statute. In *State v. Johnston*, the defendant was hired as a contractor at an optometry office to computerize the office billing system. The defendant purchased billing software and uploaded the software onto the office computers. One day, after a meeting discussing the defendant's work quality, the defendant sat down at her desk and "did something on the [computer] keyboard." The defendant then removed a box of computer diskettes from her desk and left the building.[14]

The optometrist and two other individuals immediately checked the computer and noticed that the program icon for the billing program was no longer on the computer screen. All of the patient and appointment information was missing, including demographic data, patient demographics, names, addresses, insurance types, insurance numbers, and past claims. The defendant was charged with damage to computers. The defendant was convicted of felonious damage to computers, but because the trial court failed to instruct the jury that it had to find damages in excess of $1000 for the felony conviction, the court of appeals vacated the judgment and remanded for judgment on misdemeanor damaging computers.[15]

The actions in *Johnston* are one type of activity that is subject to the statute. This statute could also apply to acts like breaking into a person's computer and deleting files, changing computer settings or passwords, introducing malware, or causing physical damage to a computer.

Denial of Computer Services and Government-Computer Services to an Authorized User

Under G.S. 14-456(a), "[a]ny person who willfully and without authorization denies or causes the denial of computer, computer program, computer system, or computer network services to an authorized user of the computer, computer program, computer system, or computer network services is guilty of a Class 1 misdemeanor." The same applies to denial of government-computer services to an authorized user and is a Class H felony under G.S. 14-456.1.

There is no North Carolina case law involving denial of computer services within the meaning of these statutes. However, other states have similar laws. In the California case *People v. Childs*, a defendant worked as the principal network engineer for a city's IT department. The department was responsible for administering the city's computer network and providing computer services to city departments, such as access to the Internet and to each department's database. The defendant, who implemented and had ownership of the city's area network, eventually locked the department out of the network. No other employees or computer experts were able to obtain administrative access to the network until the defendant revealed the access codes. This left the department unable to provide critical computer services to over sixty-five other city

14. 173 N.C. App. 334, 336 (2005) (alteration in original).
15. *Johnston*, 173 N.C. App. 334.

departments. The defendant was convicted of disrupting or denying computer services to an authorized user.[16] If similar acts were to occur in North Carolina, the perpetrator would likely be guilty of felony denial of government-computer services to an authorized user because the services were performed by a government computer.

In Delaware, "[a] person is guilty of interruption of computer services when that person, without authorization, intentionally or recklessly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized user of a computer system."[17] In *Base Optics Inc. v. Liu*, the defendant was in violation of the criminal statute when she, as an administrator, blocked a company's employees from accessing their email accounts by changing the accounts' passwords.[18]

The North Carolina statute might thus be used to prosecute cases in which a person changes passwords to a computer without authorization, where a person shuts down a network such that its users are not able to access the system or any previously available functions, or where a person unlawfully installs programs on a computer that blocks access to other programs.

Extortion

Under G.S. 14-457, anyone who maliciously threatens to "alter, damage, or destroy a computer, computer program, computer system, computer network, or any part thereof"[19] with "the intent to extort money or any pecuniary advantage, or with the intent to compel any person to do or refrain from doing any act against his will, is guilty of a Class H felony."[20]

There is no North Carolina case law related to extortion under G.S. 14-457. Extortion statutes in other jurisdictions may be instructive despite not being limited to computer-related scenarios. In a Virginia case, *DiMaio v. Commonwealth*, a defendant secured a loan from his employer that he agreed to repay by deductions from his paycheck. While still indebted to the company, the defendant announced his resignation. After announcing his resignation, the defendant transferred over 829 files from his work computer to a secure third-party server and deleted the files from his work computer. When the defendant was contacted about the missing files, he said that "he 'would be willing to provide the files to the company under the right circumstances,' namely establishing an agreement to 'return the files in exchange for forgiveness of the debt.' "[21] He was convicted of attempted extortion.

The Virginia extortion statute is not specific to computer-related crimes and thus does not require the threat to involve a computer system. Additionally, although the defendant never made a direct threat, the Virginia court reasoned that the threat of injury to the files was implied given all the surrounding circumstances, the main one being that the defendant intended to keep

16. 220 Cal. App. 4th 1079 (2013).

17. Del. Code Ann. tit. 11, § 934.

18. No. 9803-VCG, 2015 WL 3491495 (Del. Ch. May 29, 2015).

19. G.S. 14-455(a).

20. G.S. 14-457. Acts covered by this statute are likely to also be covered by G.S. 14-118.4, which punishes extortion as a Class F felony. Under the latter statute, "[a]ny person who threatens or communicates a threat or threats to another with the intention thereby wrongfully to obtain anything of value or any acquittance, advantage, or immunity is guilty of extortion."

21. 46 Va. App. 755, 761 (2005).

the information and files hostage until his $6000 debt was wiped out.[22] This reasoning leads to the possibility that a person could be charged with extortion in North Carolina under similar circumstances.

Computer Trespass

Under G.S. 14-458,

> it is unlawful for any person to use a computer or computer network without authority and with the intent to do one of any of the following:
>
> 1. Temporarily or permanently remove, halt, or otherwise disable any computer data, computer programs, or computer software from a computer or computer network.
> 2. Cause a computer to malfunction . . . .
> 3. Alter or erase any computer data, computer programs, or computer software.
> 4. Cause physical injury to the property of another.
> 5. Make or cause to be made an unauthorized copy . . . of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network.
> 6. Falsely identify with the intent to deceive or defraud the recipient or forge commercial electronic mail transmission information or other routing information . . . in connection with the transmission of unsolicited bulk commercial electronic mail through or into the computer network of an electronic mail service provider or its subscribers.[23]

The offense is a Class 3 misdemeanor. "If there is damage to the property of another and the damage caused by the prohibited acts is valued at less than [$2500]," the offense is punished as a Class 1 misdemeanor. If the damage is valued at $2500 or more, the offense is punished as a Class I felony.[24] As is the case for some of the other statutes for computer-related crimes, there is no North Carolina case law related to this offense. However, there are similar laws in other jurisdictions.

In the Georgia case *Kinslow v. State*, a defendant was convicted of one count of computer trespass. The defendant worked in the IT department of a company. Two months after the defendant's termination, it was discovered that the defendant caused internal emails intended for another IT employee to be forwarded to the defendant's personal email address. The defendant used his administrator-level access to activate this setting before his termination.[25] He was convicted for "[o]bstructing, interrupting, or in any way interfering with the use of a computer program or data"[26] in violation of Georgia's computer-trespass law.

22. *DiMaio*, 46 Va. App. 755.
23. G.S. 14-458(a).
24. G.S. 14-458(b).
25. 353 Ga. App. 839 (2020).
26. Ga. Code Ann. § 16-9-93(1) (West).

North Carolina's statute uses different language but would still apply to the defendant's acts. Forwarding internal emails without authorization falls under the category of making unauthorized copies of computer data per G.S. 14-458(a)(5), quoted above.

In a New York case, *People v. Puesan*, the defendant was convicted of computer trespass where he, without authorization, installed a keystroke-logging program on his employer's computers.[27] This could also be considered an act of making or causing to be made an unauthorized copy of computer data per G.S. 14-458(a)(5).

Limiting Language?

The computer-trespass statute begins with the language "[e]xcept as otherwise made unlawful by this Article." Although there are no cases in which this phrase is at issue, this language may be meant to limit criminal liability under this statute if one of the previously discussed offenses applies. For example, suppose a recently terminated employee deactivates or removes security software from a company's computer network. This person could likely be charged with computer trespass by means of (1) "temporarily or permanently remov[ing], halt[ing], or otherwise disabl[ing] any computer data, computer programs, or computer software from a computer or computer network" or (2) "alter[ing] or eras[ing] any computer data, computer programs, or computer software."[28] The person could also be charged with damaging computers by way of altering a computer program for those same actions. The "[e]xcept as otherwise made unlawful by this Article" language likely serves to preclude being charged with both crimes for the same act.[29] The computer-trespass statute can consequently be considered a catch-all for actions that do not fall neatly within the other statutes.

Hacking and Malware

Hacking refers to the act of gaining unauthorized or illegal access to a computer network or system. Hackers gain access to sensitive or otherwise private information by exploiting weaknesses in computer security systems. The hackers can then install ransomware or other viruses on the system. Ransomware is a type of malicious software (or *malware*) used by hackers that is designed to block access to a computer system until money is paid. Another type of malware is spyware. Spyware is a broad category of malware designed to secretly observe activity on a device. Data obtained through spyware can be used to track a user's activity online or to steal personal information, such as account passwords and credit-card numbers, which can result in identity theft and fraud.

Accessing computers, accessing government computers, damaging computers, and denying services all have another common provision. Each of these crimes applies to the introduction of a computer program (including a self-replicating or a self-propagating computer program) into a computer, computer program, computer system, or computer network to effectuate the crime. Thus, hacking by the introduction of ransomware and malware would be covered by these statutes. There is no stand-alone crime of hacking computers.

---

27. 111 A.D. 3d 222 (N.Y. App. Div. 2013).

28. G.S. 14-458(a)(1), (2).

29. Similar language in the North Carolina assault statutes has been interpreted this way. The prefatory clause "unless the conduct is covered under some other provision of law providing greater punishment" has been interpreted to mean that a defendant may be sentenced for a certain offense in the absence of an applicable greater offense, but not for both. *See* State v. Davis, 364 N.C. 297, 303 (2010); State v. Jamison, 234 N.C. App. 231, 239 (2014); State v. Fields, 374 N.C. 629, 634 (2020).

Jurisdiction

All of the cases cited previously involve scenarios in which both the victim and the defendant are in the same state and thus the same jurisdiction. However, that isn't always the case. Because these crimes can involve remote access, it is possible for a perpetrator and a victim to be located in different states.

North Carolina courts have jurisdiction over an offense if any of the "essential acts" forming the offense happened in this state.[30] More specifically, G.S. 14-453.2 provides that any offense under Article 60 "committed by the use of electronic communication may be deemed to have been committed where the electronic communication was originally sent or where it was originally received in this State." Taken together, this means that a computer crime, as defined by North Carolina law, committed out of state falls within this state's jurisdiction if the ramifications are felt within this state. Although there is no case law in which this type of jurisdiction is in question as it relates to computer crimes, other states have considered similar issues.

In a Virginia case, *Jaynes v. Commonwealth*,[31] a defendant was convicted under a provision of the Virginia Computer Crimes Act that prohibits unsolicited bulk emails. From his home in Raleigh, North Carolina, the defendant used several computers, routers, and servers to send over 10,000 emails within twenty-four hours to subscribers of AOL on each of three separate occasions. He intentionally falsified the header information[32] and sender-domain names[33] before transmitting the emails to the recipients, none of whom had requested any communication from him.

The defendant argued on appeal that the Virginia courts did not have jurisdiction over him because he did not use a computer in Virginia. The court rejected his argument, noting that the defendant knew and intended that his emails would use AOL servers because he clearly intended to send them to users whose emails ended in *@aol.com*. Additionally, the evidence established that the AOL servers were located in Virginia and that the location of AOL's servers was information easily accessible to the general public.[34]

The unsolicited-bulk-email provision in this case is similar to North Carolina's computer-trespass provision in G.S. 14-458(a)(6). This particular provision prohibits the use of a computer or computer network without authority and with the intent to "[f]alsely identify with the intent to deceive or defraud the recipient or forge commercial electronic mail transmission information

30. *See, e.g.*, State v. White, 134 N.C. App. 338, 339–40 (1999) (North Carolina had jurisdiction over heroin-trafficking offense where drugs were prepared and sold in North Carolina, even though drugs and defendant were both seized in New Jersey). The essential-acts doctrine for conferring territorial jurisdiction is codified in several statutes. *See* G.S. 15A-134 (North Carolina has jurisdiction to try an offense that occurs partly in and partly outside North Carolina); G.S. 15-131 (North Carolina has jurisdiction to try a homicide where a person is assaulted in this state but later dies in another state); G.S. 15-133 (North Carolina has jurisdiction to try a homicide where a person is assaulted outside the state but later dies in this state); G.S. 15-132 (North Carolina has jurisdiction where action taken in this state injures a person in another state).

31. 276 Va. 443 (2008).

32. In an email, the header lines identify particular routing information of the message, including the sender, recipient, date, and subject.

33. A sender domain is the domain to send emails from, which comes after the @ in the "From" address.

34. *Jaynes*, 276 Va. 443.

or other routing information in any manner in connection with the transmission of unsolicited bulk commercial electronic mail through or into the computer network of an electronic mail service provider or its subscribers." Had the defendant sent the unsolicited bulk email from his home in Virginia to users in North Carolina, he could have been charged under this statute.[35]

In an Arkansas case, *Powell v. State*, a defendant was convicted of computer fraud after receiving $15,000 from a victim of his online-romance scheme. The defendant, a resident of Georgia, met his victim, a resident of Arkansas, on a website for singles. The two engaged in lengthy email and telephone communications over the course of several months, which resulted in three face-to-face meetings in Georgia and, eventually, a marriage proposal. Throughout the course of their romance, the defendant made certain representations about himself that proved to be wholly fabricated, and ultimately he obtained about $15,000 from the victim. The defendant had never entered Arkansas until he was arrested and transported for the computer-fraud charges.[36]

The defendant argued on appeal that he was not subject to the jurisdiction of Arkansas because he only sent an email from Georgia through the network to Arkansas, the scheme was devised in Georgia, and the money was obtained in Georgia. The Arkansas court rejected his argument, reasoning that the conduct or result that was an element of the offense occurred within Arkansas. The defendant sent email correspondence to the victim and contacted her by telephone while she was in Arkansas; during the course of those communications, the defendant actively deceived the victim into sending him money; and the defendant caused the victim to access her computer, by virtue of his email correspondence, for the purpose of "[o]btaining money . . . with a false or fraudulent intent, representation, or promise."[37]

The criminal statute in this case mirrors accessing computers under G.S. 14-454, both having the same language. Thus, had the defendant committed these same acts against a North Carolina victim, the defendant could likely be charged for accessing a computer for the purpose of devising or executing any scheme or artifice to defraud.

Conclusion

Contrary to popular belief, computer crime or cybercrime does not always mean "hacking." There are various methods by which people gain unauthorized access to computers or otherwise use them to commit crimes. Our existing computer-related criminal laws encompass a wide range of those methods, and consequently will apply to a plethora of such acts. As computer crimes become more frequent, we are likely to see guidance on these laws from the appellate division in addition to any actions the General Assembly might take to address this ever-evolving area.

35. In either scenario, both states would likely have concurrent jurisdiction. On the original facts, the defendant could likely have been prosecuted under North Carolina law because the "electronic communication was originally sent" within the state. However, the prosecution is more likely to take place in the jurisdiction in which the harm is felt. Where concurrent jurisdiction exists, North Carolina has a statutory restriction dictating that it cannot try someone who has already been placed in jeopardy for the same offense by another state. G.S. 15A-134.

36. 97 Ark. App. 239 (2007).

37. Ark. Code Ann. § 5-41-103(a)(2) (West).