COLORADO COURT OF APPEALS **2016COA16**

Court of Appeals No. 14CA1207
City and County of Denver District Court No. 13CR465
Honorable Elizabeth A. Starrs, Judge

The People of the State of Colorado,

Plaintiff-Appellee,

v.

Matthew Stotz and Gustav Eicher,

Defendants-Appellants.

JUDGMENTS AND SENTENCES AFFIRMED

Division VII
Opinion by JUDGE BERGER
Richman and Dunn, JJ., concur

Announced February 11, 2016

Cynthia H. Coffman, Attorney General, Kevin E. McReynolds, Assistant Attorney General, Denver, Colorado, for Plaintiff-Appellee

Scott Robinson, P.C., Scott H. Robinson, Denver, Colorado, for Defendants-Appellants

¶ 1 Defendants, Matthew Stotz and Gustav Eicher, appeal the judgments of conviction entered on jury verdicts finding them guilty of computer crime. They also appeal the amount of restitution ordered.

¶ 2 This case requires us to determine the constitutionality of a portion of Colorado's computer crime statute providing that "[a] person commits computer crime if the person knowingly: . . . [w]ithout authorization or in excess of authorized access . . . damages . . . or causes any damage to . . . data contained in [any] computer." § 18-5.5-102(1)(e), C.R.S. 2015. We conclude that this provision is constitutional as applied to employees who a jury determined had deleted thousands of documents from their company-issued laptops, knowing that they acted without authorization or in excess of authorized access in doing so.

¶ 3 Accordingly, we affirm defendants' convictions. We also affirm the restitution orders.

I. Facts and Procedural History

A. Defendants' Employment and Resignations

¶ 4 Until their resignations in July 2012, defendants worked for the Denver office of Electric Power Systems (EPS), a nationwide

company that performs electrical testing for utilities and industrial and commercial clients. Stotz was the regional operations manager, and Eicher was the sales manager for industrial and commercial clients.

¶ 5 In the spring of 2012, defendants became unhappy with some circumstances of their employment with EPS. Along with three other Denver EPS employees, they resigned on July 23, 2012, after accepting job offers from EPC, a competitor of EPS.

B. Missing Computer Files and Alleged Damage to EPS

¶ 6 Sometime after defendants returned their company-issued laptops and left the company, EPS realized that information it needed on past, current, and potential jobs was missing from the laptops. Such information included data from the tests EPS performed on its customers' power equipment, reports on the test results that EPS prepared for its customers, the individual "test macros" or models EPS designed for each facility before testing it, bids and quotes for potential jobs, and equipment inventory and scheduling for upcoming jobs.

¶ 7 EPS employees testified that this information should have been stored on defendants' laptops for every job they had worked on

at EPS. However, Eicher's laptop contained no such information for any job, and an EPS employee testified that Stotz's laptop had incomplete information regarding some jobs. Also missing from defendants' laptops were the manuals issued by the manufacturers of the equipment being tested, which detailed the equipment's specifications, its intended use, how to install it, and when and how to maintain it.

¶ 8 Manuals were issued for each equipment model and year, and there was evidence presented at trial to support a conclusion by the jury that they were essential for performing the testing. Electrical engineers like defendants collected and kept the manuals that they used for work; for instance, Stotz testified that he uploaded over 7000 manuals to his EPS laptop when he started working there.[1]

¶ 9 EPS hired a computer forensic company to determine what had been deleted from defendants' laptops and to recover, if possible, the deleted documents. Evidence at trial showed that Stotz and Eicher had first copied files from their EPS laptops onto USB hard drives and then deleted the files from the laptops. Along

[1] The evidence reflected that some of the manuals were easy to obtain on the Internet but others, especially those for older equipment, could be more difficult to obtain.

these lines, the owner of the forensic computer company testified that he recovered 3700 deleted files and 1800 deleted e-mails from Stotz's computer and 8200 deleted files and 25,000 deleted e-mails from Eicher's computer.

C. Stotz's and Eicher's Trial Testimony

¶ 10 Both Stotz and Eicher testified at trial. Neither disputed that they copied files from their company laptops onto personal external hard drives and then deleted the files from their laptops before leaving EPS.

¶ 11 Stotz testified that he copied files so that he would have information relating to the projects he had worked on at EPS in case he needed it to protect himself from liability if a problem arose in the future with one of the projects.[2] He testified that he downloaded onto his external hard drive over 24,000 EPS files before he resigned, including 7000 manuals.

¶ 12 Stotz denied deleting any testing data or other data regarding any EPS projects from the laptop, although he admitted to deleting the 7000 manuals. He testified that he did not believe deleting the

[2] To the extent that such a justification is valid, we note that it provides an equally valid basis for EPS to retain the information.

manuals would hurt EPS because he had brought with him or obtained all the manuals himself, and he had made sure that the remaining EPS employees had copies of all the manuals he had before deleting them. He testified that most of the other files that he deleted were personal music, photo, and video files.

¶ 13 Eicher testified that only about 20% of the documents he copied and then deleted from his company laptop were EPS materials, and the remaining 80% were documents from his prior employment that he had loaded onto his EPS laptop. He claimed that he copied the EPS documents so that he would have a personal copy of his quotes and projects for his own reference in the future.

¶ 14 Regarding the deletions, Eicher testified that his understanding was that after his resignation the laptop would go to EPS's IT department and all the files on it would be erased to prepare the laptop for use by another EPS employee. He testified that he thus believed that it was not improper to erase all of the laptop's files and software other than Microsoft Word and Excel, which was the condition in which he had received the laptop when he was hired. He testified that the manuals that he deleted consisted primarily of manuals he had uploaded to the computer

when he began working for EPS. He denied that he was trying to hurt EPS by deleting them; rather, he believed that there was no need to leave the manuals on the laptop because he believed it would be wiped clean after he left.

¶ 15 Eicher testified that he deleted bids and quotes from his laptop because "deleting bids was a normal thing" for him and he deleted them as he "went along." He testified that he filed a hard copy of every bid and quote, and the information relating to every job or project, in paper folders that remained in the EPS office after he resigned. He also testified that a spreadsheet he had prepared and given to other EPS employees before leaving EPS showed every current job he was involved in and its status. He thus denied that he intended to harm EPS by deleting all his quotes, bids, and project files from the laptop because he believed that the hard copies of all the information relating to outstanding bids and past and in-progress jobs were in the office's paper files.

D. The People's Evidence

¶ 16 Although Eicher testified that he left the office's paper quote and job files organized, complete, and intact, some of the EPS employees who testified at trial disputed his assertion. For

instance, Thomas Reed, who owned EPS along with his brother Steven and their father, testified that the Denver office was missing information relating to quotes. He testified that employees consequently were not always aware of upcoming jobs and sometimes failed to show up at job sites for scheduled jobs. He also testified that because the office was missing some of the reports for jobs that had already been completed, EPS could not provide them to their customers, as required by their contracts.

¶ 17 Steven Reed likewise testified that after the resignations, Denver employees frequently did not know what jobs or quotes were pending, and they (embarrassingly) had to ask their customers to forward EPS quotes to them so that they could determine what needed to be done. And employee Michael Benitez testified that employees often did not know when and where they were scheduled to work and the specifics of the work that needed to be done, in part because the spreadsheet Eicher had provided was missing critical information. Other EPS employees gave similar testimony.

E. Civil Suit

¶ 18 EPS filed a civil suit against the five employees, including defendants, who had resigned on July 23, 2012. EPS sought to

enforce the noncompete agreements each employee had entered into with EPS and to obtain money damages. Following a preliminary injunction hearing in October 2012, the district court mainly denied relief to EPS, concluding that the noncompete agreements were probably unenforceable. The court also determined that EPS probably could not establish that any data or documents in the possession of the civil defendants had been provided to EPC to the detriment of EPS.

¶ 19 The court did grant a limited preliminary injunction, enjoining, for a period of time, the civil defendants from using information pertaining to bids they had been working on at EPS, and from submitting further bids on behalf of EPC for projects they worked on at EPS. The court also ordered the civil defendants to return to EPS all the documents and data that they had downloaded to hard drives. However, it is undisputed that defendants had already done so about a month earlier, in September 2012, approximately six weeks after their resignations.

F. Criminal Charges

¶ 20 In November 2012, EPS submitted a formal complaint to the Economic Crime Unit of the Denver District Attorney's (DA's) office,

seeking criminal prosecution of defendants. The DA's office filed criminal charges against defendants in January 2013. At some point before trial, EPS sought and obtained, over the objection of all the civil defendants, dismissal without prejudice of the civil suit.

¶ 21 Defendants were charged with computer crime, causing loss of $1000 or more but less than $20,000; conspiracy to commit computer crime; conspiracy to commit theft; theft of trade secrets; and conspiracy to commit theft of trade secrets. A jury convicted defendants of felony computer crime but acquitted them of the other charges.[3] The trial court sentenced defendants to a two-year suspended prison sentence, imposed two years' probation, and awarded EPS $104,920.26 in restitution, for which defendants are jointly and severally liable.

II. Computer Crime Statute

[3] Defendants were convicted under a prior version of section 18-5.5-102(3)(a), which provided that computer crime causing loss of $1000 or more but less than $20,000 was a class 4 felony. Ch. 384, sec. 14, § 18-5.5-102(3)(a), 2007 Colo. Sess. Laws 1696. In 2014, the General Assembly amended the statute, and it now provides that computer crime causing loss of $750 or more but less than $2000 is a class 1 misdemeanor, $2000 or more but less than $5000 is a class 6 felony, and $5000 or more but less than $20,000 is a class 5 felony. § 18-5.5-102(3)(a)(IV), (V), (VI), C.R.S. 2015.

¶ 22 Defendants argue that the computer crime statute under which they were convicted is unconstitutional on its face and as applied to them because it (1) provides inadequate guidance regarding what conduct is prohibited and thus is void for vagueness; (2) criminalizes lawful conduct and thus is unconstitutionally overbroad; and (3) under *People v. Vinnola*, 177 Colo. 405, 494 P.2d 826 (1972), impermissibly left the determination of their criminality to EPS. We reject defendants' arguments.

¶ 23 The parties agree that defendants preserved their arguments by moving pretrial for an order declaring the statute unconstitutional on the same grounds as those asserted on appeal. The trial court denied the motion.

¶ 24 We review de novo a constitutional challenge to a statute. *People v. Cisneros*, 2014 COA 49, ¶ 23. Statutes are presumed to be constitutional, and the party challenging the statute has a heavy burden to establish that it is unconstitutional. *See id.*

A. Vagueness

1. Law

¶ 25 Due process "requires that a penal statute define [a] criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." *Kolender v. Lawson*, 461 U.S. 352, 357 (1983); *see also People v. Gross*, 830 P.2d 933, 937 (Colo. 1992). A statute is unconstitutionally vague under the void-for-vagueness doctrine if it "fail[s] to provide the kind of notice that will enable . . . . the ordinary citizen to conform his or her conduct to the law," *City of Chicago v. Morales*, 527 U.S. 41, 56, 58 (1999), or "its standards are so ill-defined as to create a danger of arbitrary and capricious enforcement," *People v. Shell*, 148 P.3d 162, 172 (Colo. 2006).

¶ 26 Thus, in addressing a void for vagueness challenge, we must determine "whether the statute 'forbids or requires the doing of an act in terms so vague that persons of ordinary intelligence must necessarily guess as to its meaning and differ as to its application.'" *Gross*, 830 P.2d at 937 (quoting *People v. Becker*, 759 P.2d 26, 31 (Colo. 1988)).

¶ 27 A statute may be challenged as unconstitutionally vague either on its face or as applied to particular conduct. *People v. Devorss*,

277 P.3d 829, 835 (Colo. App. 2011). A statute is unconstitutionally vague on its face if it is incomprehensible in all of its applications. *Shell*, 148 P.3d at 172. A statute is unconstitutionally vague as applied if it does not, with sufficient clarity, prohibit the conduct against which it is enforced. *Devorss*, 277 P.3d at 835. If a defendant's conduct is clearly proscribed by the statute — that is, the statute is not vague as applied to the defendant's conduct — the defendant cannot successfully challenge the vagueness of the law on its face or as applied to the conduct of others. *See People v. Perea*, 74 P.3d 326, 332 (Colo. App. 2002).

¶ 28 We apply familiar principles of statutory interpretation in analyzing a vagueness challenge. Our primary task is to ascertain and give effect to the intent of the legislature. *Whimbush v. People*, 869 P.2d 1245, 1249 (Colo. 1994). "To determine legislative intent, we begin with the language of the statute itself and interpret statutory terms in accordance with their commonly accepted meanings." *Id.* If the plain language of the statute is clear and unambiguous, we must apply it as written. *People v. Goodale*, 78 P.3d 1103, 1107 (Colo. 2003). "Only when the statute is unclear or

ambiguous may we look beyond the words of the statute to legislative history or rules of statutory construction." *Id.*

2. Application

¶ 29 The section of the computer crime statute under which defendants were convicted provides:

> A person commits computer crime if the person knowingly: . . . (e) Without authorization or in excess of authorized access alters, damages, interrupts, or causes the interruption or impairment of the proper functioning of, or causes any damage to, any computer, computer network, computer system, computer software, program, application, documentation, or data contained in such computer, computer network, or computer system or any part thereof.

§ 18-5.5-102(1).

¶ 30 The terms "authorization," "in excess of authorized access," and "damage" are defined by statute:

> (1) "Authorization" means the express consent of a person which may include an employee's job description to use said person's computer, computer network, computer program, computer software, computer system, property, or services as those terms are defined in this section.
> . . . .
> (6.3) "Damage" includes, but is not limited to, any impairment to the integrity of availability of information, data, computer

> program, computer software, or services on or via a computer, computer network, or computer system or part thereof.
>
> (6.7) "Exceed authorized access" means to access a computer with authorization and to use such access to obtain or alter information, data, computer program, or computer software that the person is not entitled to so obtain or alter.

§ 18-5.5-101, C.R.S. 2015.[4]

¶ 31 The jury was instructed on the statutory definitions of these terms and the elements of computer crime.

¶ 32 First, we conclude that the term "knowingly" in section 18-5.5-102(1)(e) applies to every element of the offense. "When a statute defining an offense prescribes as an element thereof a specified culpable mental state, that mental state is deemed to apply to every element of the offense unless an intent to limit its application clearly appears." § 18-1-503(4), C.R.S. 2015. Because the term

---

[4] No published appellate decision from Colorado specifically addresses the constitutionality of section 18-5.5-102(1)(e), although a division of this court has held that applying the plain and ordinary meaning to the term "access" as it is used in sections 18-5.5-102(1)(c)-(d) did not render those sections unconstitutionally vague. *People v. Rice*, 198 P.3d 1241, 1245 (Colo. App. 2008). A division of this court also has held that the term "computer," as used in a prior version of sections 18-5.5-102(1)(c)-(d), is readily understandable by an ordinary person of reasonable intelligence. *People v. Pahl*, 169 P.3d 169, 187 (Colo. App. 2006).

"knowingly" in section 18-5.5-102(1)(e) is placed immediately before a colon establishing the elements of the crime, we must assume that the General Assembly intended the term to modify every element of the offense; no contrary legislative intent clearly appears. Accordingly, a person commits computer crime under the statute if he knowingly commits one of the statute's proscribed acts knowing that he does so "[w]ithout authorization or in excess of authorized access." *See* § 18-5.5-102(1)(e).

a. Facial Challenge

¶ 33 Defendants argue that section 18-5.5-102(1)(e) is void on its face because the phrase "causes any damage to . . . data contained in [a] computer" is not adequately concrete to reasonably forewarn persons of ordinary intelligence of what is prohibited. We disagree.

¶ 34 "A law is unconstitutionally vague only if it specifies no standard of conduct at all, and not if it requires a person to conform his or her conduct to an imprecise, but comprehensible normative standard." *Perea*, 74 P.3d at 332.

¶ 35 The deletion of thousands of documents from one's employer's laptop clearly falls within the statutory definition of "damage." § 18-5.5-101(6.3). The definition of damage is specific enough to

provide a person of ordinary intelligence notice that the deletion of documents from a computer may cause damage to data contained in a computer. *See Shell*, 148 P.3d at 173. Therefore, defendants have not established that the statute is incomprehensible in all of its applications. *See id.* at 172; *see also People v. McCoy*, 2015 COA 76M, ¶¶ 58-66 (concluding that the "incomprehensible in all applications" standard remains good law, notwithstanding *Johnson v. United States*, 576 U.S. ___, ___, 135 S. Ct. 2251, 2561 (2015)).

¶ 36 Defendants express doubts regarding whether an individual actually "damaged" data under the statute when the data was placed on the computers by the individuals themselves and hard copies of the deleted information were stored in a physical location. However, this was a factual issue for the jury to resolve; the plain language of the statute gives sufficient fair warning that "impairing the integrity of availability of information [or] data" covers deleting documents from a company laptop such "that persons may guide their actions accordingly." *See Gross*, 830 P.2d at 937.[5]

[5] Defendants do not challenge on appeal the sufficiency of the evidence to support their convictions.

¶ 37 Defendants also worry that because there is no malicious intent requirement in section 18-5.5-102(1)(e), if the statute is permissibly applied to a situation like theirs, any keystroke knowingly made by an employee on a company computer that alters content on that computer could form the basis for criminal charges. But in interpreting a statute, it must "be considered and read as a whole." *People v. Randolph*, 852 P.2d 1282, 1284 (Colo. App. 1992). The statute interpreted as a whole does not proscribe any keystroke that changes or deletes content on a computer; it only proscribes such an act if it is done knowingly without authorization or in excess of authorized access *and* with knowledge that it will impair "the integrity of availability of information, data, computer program, computer software, or services on or via a computer, computer network, or computer system or part thereof." *See* §§ 18-5.5-101, 18-5.5-102(6.3).

¶ 38 Accordingly, defendants' facial challenge to section 18-5.5-102(1)(e) based on the term "damage" fails.

b. As-Applied Challenge

¶ 39 Defendants argue that the statute is vague as applied to their actions because (1) they had full authority over their own laptops,

and management neither exercised any control, nor promulgated any rules or guidelines, over the placement, retention, or deletion of the content of their laptops; (2) the legislative intent of the computer crime statute was to criminalize hacking and the use of a computer to commit fraud and embezzlement, not to prosecute employees for data deletion decisions; and (3) as demonstrated by out-of-state cases, the statute provides insufficient notice that it reaches employees' acts with respect to information on a computer that the employees had authority to access.

i. Authorization

¶ 40 Much of defendants' vague-as-applied argument focuses on the fact that EPS's employee handbook provided that "[l]ocal administrative rights and support of standard EPS hardware or software shall be granted to all employees," and testimony by defendants and other former and current EPS employees that EPS employees had full authority over the content of their laptops.

¶ 41 For example, Stotz testified that he had never received, nor believed that he needed to receive, prior authorization before downloading, uploading, or deleting documents from his computer, and that EPS never advised him regarding what he could or could

not delete from his computer. He testified that, to him, "local administrative rights" meant that he could do what he wanted with his computer.

¶ 42 Eicher similarly testified that he alone decided what to put on his laptop the entire time he worked for EPS, and there was no direct supervisory input, direction, or oversight from management or anyone else regarding what he should or should not do with his laptop. His understanding was that he had complete autonomy in adding, copying, or deleting material to or from his laptop.

¶ 43 Other former and current EPS employees provided similar testimony about decision-making authority over company laptops. Steven Reed, for example, testified that an employee did not need advance permission to download a document onto an EPS computer, and that no one at EPS supervised employees' day-to-day decisions about what to put on, or delete from, their computers.

¶ 44 Nevertheless, the prosecution's theory of liability at trial was that defendants knew that they were not authorized to delete the documents they deleted from their laptops at the time that they deleted them. To this end, Steven Reed testified that he had never authorized defendants to delete reports, records, test results,

quotes, and the like from EPS's computers or computer networks. Thomas Reed also testified that he had never authorized defendants to delete that type of material from their computers, and that he never would have done so because maintaining that information was critical for EPS's business. During cross-examination, Stotz admitted that nobody authorized him to delete the files at issue, and that he did not ask permission before doing so. Eicher testified that nobody ever authorized him to delete EPS files.

¶ 45 The prosecution also adduced a significant amount of testimony on a data storage program called "SharePoint" that EPS's Denver office used. Steven Reed testified that in January 2012, EPS management informed all offices that they were to start using a central drive to store their critical data. However, the management group in Denver, including Stotz, told Steven Reed that they were more comfortable using SharePoint for central data storage, and an agreement was reached between EPS management and the Denver office in April 2012 that all managers in Denver would save their information to SharePoint rather than the central drive.

¶ 46 But from April until defendants' resignations in July 2012, no documents from the Denver office were saved to SharePoint.

Defendants and other Denver employees testified that SharePoint stopped working in April, and they were unable to save information to it from that point forward. The prosecution presented testimony from EPS employees that would permit the jury to infer that if it was true that SharePoint had not been working, the only reason defendants would have deleted critical information from their laptops was to harm EPS by destroying the only electronic copy of that information.

¶ 47 We conclude that the plain language of section 18-5.5-102(1)(e) prohibits, with sufficient clarity, an employee's knowing deletion of the only electronic copies of thousands of computer documents, when the employee knows that such deletion is not authorized by the employer. *See Devorss*, 277 P.3d at 835.

¶ 48 Although defendants had authority to access the documents they deleted, the jury necessarily determined that they exceeded such authorized access by deleting information that they were not authorized to delete. Accordingly, defendants' acts fall squarely within the statute's proscription of accessing a computer with authorization and using such access to knowingly damage

information on the computer, knowing that they were not entitled to do so. *See* § 18-5.5-101(6.7).

¶ 49 Defendants' argument essentially boils down to an assertion that, under all the circumstances, they did not know, and reasonably could not have known, that they were not entitled to delete the documents. But the truth of this assertion was a factual question for the jury; it is not a proper basis for us to conclude that the statute does not provide fair notice that it forbids an employee from knowingly deleting files from a company computer, knowing that he did not have authorization to do so.

ii. Legislative History

¶ 50 We do not consider defendants' argument that the General Assembly did not intend section 18-5.5-102(1)(e) to be applied in cases such as this because, according to defendants, the General Assembly only intended the statute to permit prosecution of hackers, individuals who commit theft or fraud through the use of a computer, and those who introduce viruses onto a computer to damage its software or data. Because the plain language of the statute is clear and unambiguous, we may not look beyond the words of the statute to determine the General Assembly's intent in

enacting it. *See Goodale*, 78 P.3d at 1107; *see also* § 2-4-203, C.R.S. 2015 (identifying aids in construction that can be applied *if* a statute is ambiguous).

¶ 51 Thus, even if the legislative history does show, as defendants claim it does, that the statute was not intended to permit prosecution under the circumstances here, because the statute's plain and ordinary language applies to defendants' conduct, we will not second guess whether the General Assembly intended such an outcome. "[I]t is not the role of [the] court[s] to act as overseer[s] of all legislative action and declare statutes unconstitutional merely because we believe they could be drafted better or more fairly applied." *Id.* at 1105-06 (citation omitted).

iii. Federal and Out-of-State Authority

¶ 52 Defendants cite a number of federal and out-of-state cases that have held that state or federal computer crime statutes do not criminalize similar acts taken by employees on their employer's computers. The People, conversely, cite other cases in which computer crime statutes *were* held to criminalize similar employee conduct. However, most of the cases cited both by defendants and the People are inapposite.

¶ 53 Many of the statutes at issue in those cases proscribe unauthorized access or access in excess of authorized access, but they do not require, like section 18-5.5-102(1)(e) does, that the actor "know" his actions are unauthorized. Moreover, unlike section 18-5.5-102(1)(e), some of those statutes punish simple access; there is no additional requirement that the actor commit an act that alters or damages the computer or information on it. Consequently, applying section 18-5.5-102(1)(e) to defendants' conduct here does not engender the same vagueness problems that other courts have concluded may arise with criminalizing mere unauthorized access.

¶ 54 Most of the federal cases cited by the parties address a provision of the federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (2012), that proscribes certain acts taken in connection with the intentional or knowing access of a computer without authorization or in excess of authorized access. *See, e.g.*, *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1131 (9th Cir. 2009). The federal circuits are split over the applicability of that provision to circumstances such as those in this case.

¶ 55 One line of cases holds that if an employee had authority to access a computer owned by his employer, and moreover had authority to access certain information on that computer, the employee did not violate the statute by copying, deleting, transmitting, altering, or taking any other action with respect to that information. *See, e.g.*, *United States v. Nosal*, 676 F.3d 854, 864 (9th Cir. 2012); *LVRC Holdings*, 581 F.3d at 1135; *United States v. Aleynikov*, 737 F. Supp. 2d 173, 194 (S.D.N.Y. 2010). These cases emphasize that "[t]he phrases 'accesses a computer without authorization' and 'exceeds authorized access' cannot be read to encompass an individual's misuse or misappropriation of information to which the individual was permitted access." *Aleynikov*, 737 F. Supp. 2d at 192. As the Southern District of New York put it, "[w]hat use an individual makes of the accessed information is utterly distinct from whether the access was authorized in the first place." *Id.*

¶ 56 Applying various rules of construction, including the rule of lenity, courts in this line of cases have concluded that the language of the provision prohibits only unauthorized access of computer information, not its misuse or misappropriation. *See Nosal*, 676

F.3d at 862-63 (discussing the rule of lenity and collecting cases); *see also United States v. Valle*, 807 F.3d 508, 523-28 (2d Cir. 2015); *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 203-07 (4th Cir. 2012).

¶ 57 Another line of CFAA unauthorized access cases reaches the opposite result, holding that an employee with authority to access his employer's computer and certain documents on that computer who takes action with respect to those documents that constitutes a breach of his duty of loyalty to his employer terminates his agency relationship with his employer. *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006). The termination of the agency relationship terminates the employee's authority to access the computer and the documents, and thus the employee's action in violation of his duty of loyalty — such as deleting data on the computer that the employee knows that the employer would want to save — constitutes access without authorization or in excess of authorized access. *Id.* at 421; *see also United States v. Rodriguez*, 628 F.3d 1258, 1263-64 (11th Cir. 2010); *United States v. John*, 597 F.3d 263, 271-73 (5th Cir. 2010).

¶ 58 Many of the state cases cited by defendants also address statutes that proscribe unauthorized access. *See, e.g.*, *Briggs v. State*, 704 A.2d 904, 907 (Md. 1998); *State v. Riley*, 988 A.2d 1252, 1257 (N.J. Super. Ct. Law Div. 2009); *People v. Klapper*, 902 N.Y.S.2d 305, 308 (N.Y. Crim. Ct. 2010); *State v. Olson*, 735 P.2d 1362, 1363 (Wash. Ct. App. 1987). Like the first line of federal cases discussed above, these cases hold that the state statutes at issue apply to employees who act in excess of their authorization to *access* a computer or data on the computer, but the statutes do not apply to those who have access to the computer or data but act in excess of their authorization in how they *use* the computer or data. *Riley*, 988 A.2d at 1259; *see also Briggs*, 704 A.2d at 909-10; *Olson*, 735 P.2d at 1364-65.

¶ 59 Courts that are reluctant to extend the reach of unauthorized access statutes to proscribe the type of conduct in this case emphasize that doing so "would expand [the statute's] scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer" and "would make criminals of large groups of people who would have little reason to suspect they are committing a . . . crime." *Nosal*, 676 F.3d at 859.

¶ 60 For example, the Ninth Circuit has explained that if the CFAA's unauthorized access provision is interpreted to refer to an employee who has authority to access a computer or certain information on it but his use of that information violates his employer's computer policy, any use by the employee of his computer in violation of the computer use policy would become a crime. *Id.* at 860. The Ninth Circuit emphasized that "[s]ignificant notice problems arise if we allow criminal liability to turn on the vagaries of private policies that are lengthy, opaque, subject to change and seldom read." *Id.*; *see also Riley*, 988 A.2d at 1264-67.

¶ 61 But as we have previously discussed, the plain language of section 18-5.5-102(1)(e) does proscribe defendants' conduct, and we are not at liberty to limit or rewrite the statute merely because the General Assembly may not have "intended the consequences of its enactment[]." *People v. Cooper*, 27 P.3d 348, 360 (Colo. 2001).

¶ 62 Moreover, applying section 18-5.5-102(1)(e) under the circumstances of this case does not create the same danger perceived by the Ninth Circuit and other courts of applying unauthorized access statutes in similar circumstances. Unlike section 18-5.5-102(1)(2), those statutes proscribe unauthorized

access to a computer or information on the computer, but do not apply any culpable mental state requirement to the "unauthorized" element. *See, e.g.*, *id.* at 859.

¶ 63 Because section 18-5.5-102(1)(e) criminalizes only "knowing" unauthorized access or access in excess of authorized access, the same is not true here. An employee who did not know that his actions were unauthorized could not be liable under the statute, and thus the same notice issues detailed in *Nosal* and similar cases do not arise.

¶ 64 Also, section 18-5.5-102(1)(e) does not criminalize mere unauthorized access. Rather, it criminalizes the *combination* of unauthorized access or access in excess of authorization with the knowing taking of an additional unauthorized action (altering, damaging, interrupting, or impairing) with respect to the computer or computer network accessed, or the program, document, or data contained on that computer or network. *See* § 18-5.5-102(1)(e); *see also B&B Microscopes v. Armogida*, 532 F. Supp. 2d 744, 757-58 (W.D. Pa. 2007) (Under another CFAA section that proscribes using unauthorized access to a computer to "knowingly cause[] the transmission of a program, information, code, or command, and as

a result of such conduct, intentionally cause[] damage without authorization, to a protected computer," liability is "not predicated upon unauthorized access of a protected computer," but rather "*unauthorized damage* to a computer.") (emphasis added).

¶ 65 Thus, although "a person of common intelligence [might] not be reasonably apprised that it is a serious crime to violate internal workplace policies on using computers to which the employee has [authorized access]," *Riley*, 988 A.2d at 1265, the same cannot be said when committing the crime requires knowingly committing another action beyond the mere access of the computer or information on the computer, knowing that the taking of such an action is unauthorized. *See* § 18-5.5-102(1)(e). This requirement of an additional action reduces the concern of arbitrary enforcement — that the state would be empowered, "unguided by firm definitional standards, to choose to prosecute whomever it wishes from [the] broad cross-section of the population" that consists of employees who violate internal workplace computer use policies. *See Riley*, 988 A.2d at 1266.[6]

[6] Defendants also cite two state cases in which a State's computer crime statute was held to be unconstitutionally vague. *See*

¶ 66 For all these reasons, section 18-5.5-102(1)(e), as applied to defendants' conduct, does, "with sufficient clarity, prohibit the conduct against which it is to be enforced," *People v. Couillard*, 131 P.3d 1146, 1151 (Colo. App. 2005), and it is not void for vagueness.[7]

B. Overbreadth

¶ 67 Defendants argue that applying section 18-5.5-102(1)(e) to their conduct, on the theory that they caused damage to data on

---

Commonwealth v. Cocke, 58 S.W.3d 891 (Ky. Ct. App. 2001); *State v. Azar*, 539 So. 2d 1222 (La. 1989). The provision of Colorado's computer crime statute at issue here does not suffer from the same defects of the statutes addressed in those cases. *See Cocke*, 58 S.W.3d at 894 ("[A]bsent a requirement that the actor's alteration, damage or destruction must occur without authorization, the [Kentucky statute at issue] literally permits the prosecution of an authorized user for an alteration as innocuous and innocent as the deletion of an e-mail message."); *Azar*, 539 So. 2d at 1224-26 (no mens rea requirement applicable to the element of "alteration, deletion, or insertion of programs or data").

[7] Although we have determined that section 18-5.5-102(1)(e) is not unconstitutional on its face or as applied to defendants, we acknowledge that the statute is subject to potential abuse. Because the statutory language is clear and unambiguous, we must presume that the "General Assembly meant what it clearly said" and apply the statute as written. *Robbins v. People*, 107 P.3d 384, 391 (Colo. 2005) (citation omitted); *People v. Lassek*, 122 P.3d 1029, 1032 (Colo. App. 2005). However, if the General Assembly in fact did not intend the statute to apply to circumstances such as those here, "it is free to amend the [statute] as it sees fit." *Leonard v. McMorris*, 63 P.3d 323, 339 (Colo. 2003) (Mullarkey, C.J., dissenting).

their laptops in excess of authorized access, punishes legitimate activity — the exercise of permitted discretion by an employee — and thus the statute is unconstitutionally overbroad. We disagree.

¶ 68 A statute is overbroad if "it sweeps within its reach constitutionally protected, as well as unprotected, activities." *Cisneros*, ¶ 39. "A penal statute is . . . said to be overbroad if it prohibits activity that is legitimate, in the sense that it cannot be proscribed by exercise of the State's police power." *Gross*, 830 P.2d at 939. The proscription of an act is within the State's police power if it is reasonably related to a legitimate governmental interest, such as the protection of the public health, welfare, and safety. *Id.*; *People v. Smith*, 638 P.2d 1, 7 (Colo. 1981).

¶ 69 Although defendants emphasize that they themselves placed on the computers the documents that they ultimately deleted, EPS's employee handbook makes clear that "[a]ll computer disks, computer software programs, computer records, and computer files and documents provided to [employees] or *created by* [employees] during [their] employment with [EPS] are the exclusive property of [EPS]." (Emphasis added.) Thus, as applied to defendants, section 18-5.5-102(1)(e) proscribes knowingly damaging EPS's property,

knowing that they had no permission to do so. Such conduct is undoubtedly within the power of the State to regulate because protecting an individual's private property serves to protect the public welfare. *See Smith*, 638 P.2d at 7.

¶ 70 Defendants argue that criminalizing an employee's deletion of data from a company computer that the employer claims it wanted to remain on the computer would punish countless day-to-day decisions made by employees throughout Colorado. But except in the context of the First Amendment, "a person to whom a statute was constitutionally applied will not be heard to challenge that statute on the ground that it may conceivably be applied unconstitutionally to others, in other situations not before the [c]ourt." *Cisneros*, ¶ 39 (citation omitted); *see also Bolles v. People*, 189 Colo. 394, 396, 541 P.2d 80, 82 (1975) (First Amendment exception). Because section 18-5.5-102(1)(e) constitutionally applies to defendants, we do not consider whether there are other circumstances in which the statute could not be constitutionally applied because its application would prohibit legitimate acts.

¶ 71 Accordingly, we reject defendants' overbreadth challenge.

C. *Vinnola*

¶ 72 In *People v. Vinnola*, the supreme court invalidated a statute that included a provision proscribing uttering or passing a check "knowing or having reasonable cause to know at the time of uttering [or passing] it that it will not be paid, and it is not paid because of insufficient funds." 177 Colo. at 407, 411, 494 P.2d at 827, 829. The supreme court concluded that the statute was unconstitutional in part because "criminal liability and punishments should not be predicated upon a third party's unfettered discretion":

> [U]nder the various provisions of [the statute], the action of a third party, the bank, can often be the factor which determines whether guilt attaches. If two customers each write a check knowing it will not be paid on presentment due to insufficiency of funds in their respective accounts, each should be theoretically guilty of a crime. Yet, the bank upon which the check is drawn has the discretion to dishonor one and pay the other. Such a discretion is at odds with constitutional due process and equal protection of the laws.

Id. at 416, 494 P.2d at 831.

¶ 73 Defendants argue that, likewise, the application of section 18-5.5-102(1)(e) to their conduct permitted a third party — EPS — to determine in its unbridled discretion whether a crime had been committed. Defendants assert that their convictions were based on

the testimony of EPS executives that the deletions were unauthorized, and thus a third party had the discretion to decide, after the fact, whether guilt should attach to their actions. We disagree.

¶ 74 The determination whether defendants had authorization to delete the files depended on the state of facts as they existed *when* defendants deleted the files. The jury had to determine whether defendants had authorization to take that action *at that time*. Consequently, when EPS executives testified that defendants were not authorized to delete the files, the facts supporting the alleged crime had already been fixed; its commission did not depend on decisions the executives made after the fact. Instead, the testimony went to the issue of proof.

¶ 75 This case thus is different from *Vinnola* because in that case, "the [defendant's] conduct was complete prior to the time the disinterested third party bank had the complete freedom to decide whether to honor or dishonor the insufficient funds check," and the crime was not committed unless the bank decided to dishonor the check. *Smith*, 638 P.2d at 6.

¶ 76 Applying section 18-5.5-102(1)(e) under the circumstances here "does not condition criminal responsibility on the action of a third party after the prohibited conduct already has occurred." *People v. Andrews*, 632 P.2d 1012, 1016 (Colo. 1981). Rather, the statute's application to defendants' conduct is analogous to that in *Smith*, in which the supreme court held that the second degree sexual assault statute was not constitutionally deficient merely because of the "victim's ability to characterize his or her own conduct as consensual or nonconsensual after the incident has occurred." *Smith*, 638 P.2d at 6-7. "This is simply a problem of proof. Whether consent existed at the relevant time is an objective fact, not something which can be varied by a later decision of the victim." *Id.* at 7.

¶ 77 Accordingly, we reject defendants' argument that application of section 18-5.5-102(1)(e) to their conduct unconstitutionally permitted EPS to determine whether they had committed a crime.

III. Restitution

A. Additional Facts

¶ 78 About six weeks after their resignations, defendants returned to EPS the information that they had copied from their laptops.

Several EPS employees, including Steven and Thomas Reed, Benitez, and John Poole, testified at trial that, until defendants did so, the lack of critical information on defendants' laptops, SharePoint, and in the hard copy files impeded EPS's operation of its business. The employees explained that although the computer forensic company provided EPS with data recovered from the deleted files on defendants' laptops about a week after the resignations, the data consisted of one long string of documents in which it was difficult to find information.[8] Also, some of the information was corrupted. Consequently, EPS employees spent many hours looking for information related to EPS jobs, projects, and proposals, and attempting to recreate or obtain information that was missing.

---

[8] This information included only those files that the computer forensic company was able to recover from defendants' laptops. EPS employees testified that when, about five weeks later, defendants provided EPS with copies of the hard drives onto which they had copied the contents of their laptops before they had deleted the files, it became clear that the forensic computer company had not been able to recover all of the deleted information. Moreover, the documents provided by defendants six weeks after their resignations were organized and labeled how the testifying EPS employees expected, thus allowing them to easily find what they needed, whereas the recovered documents provided by the forensic computer company were not.

¶ 79 Also admitted at trial was Exhibit 121, which consisted of EPS employee time sheets showing how much time each employee worked on problems caused by the file deletions. After defendants were convicted, EPS completed a victim impact statement showing a total financial loss to EPS of $126,371, which included $92,711 in employee compensation. Attached to the victim impact statement was a chart showing the total hours worked by each employee in response to defendants' criminal acts and the employee's hourly wage and benefits.

¶ 80 At defendants' sentencing, the prosecution requested $130,574.50 in restitution. Defendants objected, and the trial court set a restitution hearing.

¶ 81 At the restitution hearing, Thomas Reed testified that he and the prosecutor had gone over the chart attached to the victim impact statement and determined that it contained some errors. As a result, in preparing the restitution request for the hearing, they created Exhibit 1, which purportedly corrected the errors, removed employee time that was not directly related to defendants' criminal conduct, and accurately reflected the hours employees worked on problems caused by the deletions. Based on Exhibit 1, the

prosecution requested $84,401.67 in restitution for employee compensation, with $58,193.67 reflecting the amount of compensation owed for time employees spent working on such problems (the remaining amount reflected employee time spent preparing for the criminal trial).

¶ 82 The trial court found that the time shown in Exhibit 1 was a reasonable amount of time spent on the recovery of documents, but it still did not grant the full amount requested because there was no evidence that EPS paid the employees listed in Exhibit 1 for any work in excess of forty hours a week. The court thus limited each employee's recoverable salary time to forty hours a week, and it awarded $51,181.78 in restitution to EPS for employee costs associated with time spent recovering the documents.[9]

B. Law and Application

¶ 83 Defendants argue that the trial court erred in the amount of restitution it awarded because (1) the court refused to take into

[9] The trial court also awarded restitution for the costs EPS incurred relating to the hiring of the computer forensic company and those it incurred in preparing for the criminal trial. The court further awarded to the People costs incurred by the DA's office in prosecuting the case. Defendants do not specifically challenge on appeal any of these awarded amounts.

account that the amount of loss found by the jury was less than $20,000; (2) the court's award of employee costs relied on exaggerated and false exhibits and testimony presented by EPS representatives; and (3) the prosecution made no effort to apportion employee time attributable to doing the work of the departed employees from the time allegedly spent dealing with the data deletions. We conclude that the trial court did not abuse its discretion in determining the amount of restitution owed.

¶ 84 The parties agree that defendants preserved their arguments on restitution.

¶ 85 A trial court has broad discretion to determine the terms and conditions of a restitution order, and its ruling will not be disturbed absent an abuse of discretion. *People v. Reyes*, 166 P.3d 301, 302 (Colo. App. 2007). A court abuses its discretion when it misconstrues or misapplies the law, *id.*, or when its decision fixing the amount of restitution is not supported by the record, *see People v. Rivera*, 968 P.2d 1061, 1068 (Colo. App. 1997). "We will not disturb the [trial] court's determination as to the proper amount of restitution if it is supported by the record." *People v. Bohn*, 2015 COA 178, ¶ 8.

¶ 86 As part of "[e]very order of conviction," a trial court must order a defendant to pay restitution if the defendant's conduct caused pecuniary loss to a victim. § 18-1.3-603(1), C.R.S. 2015; *see also Reyes*, 166 P.3d at 302. "'Restitution' means any pecuniary loss suffered by a victim and includes but is not limited to all out-of-pocket expenses, interest, loss of use of money . . . and other losses or injuries proximately caused by an offender's conduct and that can be reasonably calculated and recompensed in money." § 18-1.3-602(3)(a), C.R.S. 2015. "[P]roximate cause" is defined as "a cause which in natural and probable sequence produced the claimed injury and without which the claimed injury would not have been sustained." *Reyes*, 166 P.3d at 303 (citation omitted). The prosecution bears the burden of proving the amount of restitution owed by a preponderance of the evidence. *People v. Pagan*, 165 P.3d 724, 729 (Colo. App. 2006).

¶ 87 At the restitution hearing, Thomas Reed testified that Exhibit 1 was an accurate representation of the time he, his brother, Poole, and Benitez worked on problems caused by defendants' crimes and that but for the crimes, those employees would not have spent that time doing that work. He further testified that he believed that the

amount of time shown in Exhibit 1 as hours each employee spent working on such problems was accurate because the employees had entered those hours on time sheets they submitted to EPS as time spent working on those problems.

¶ 88 This testimony, along with supporting exhibits, is sufficient to support the trial court's award. The value of an employee's time constitutes "actual pecuniary damages" sustained by a victim company, and the value of such time is appropriately included in a restitution award, regardless of whether any funds in addition to the employee's regular salary were expended by the victim company. *People v. Duvall*, 908 P.2d 1178, 1180 (Colo. App. 1995); *see also People v. Witt*, 15 P.3d 1109, 1111 (Colo. App. 2000) ("[T]he value of employees' time spent on tasks made necessary by a defendant's conduct is compensable."). Accordingly, the value of the hours that EPS employees worked on problems caused by defendants' criminal acts constituted a pecuniary loss suffered by EPS. *See Witt*, 15 P.3d at 1111; *Duvall*, 908 P.2d at 1180.

¶ 89 Defendants argue that the trial court abused its discretion in not considering the jury's verdict in determining the applicable restitution. The trial court rejected this argument, concluding that

the jury's verdict that defendants committed computer crime causing a loss of more than $1000 but less than $20,000 did not limit the restitution amount to less than $20,000. The court based its conclusion on cases from this court that hold that a jury verdict establishing that a defendant's crime caused a certain amount of loss does not limit the amount of restitution to that amount or less. *See People v. Smith*, 181 P.3d 324 (Colo. App. 2007); *Pagan*, 165 P.3d 724.

¶ 90 One of the reasons for this rule is that in determining the proper amount of restitution owed, sentencing courts may consider both uncharged and acquitted criminal conduct that has been proved by a preponderance of the evidence; courts are not limited to considering only the criminal conduct which a defendant was found beyond a reasonable doubt to have committed. *Smith*, 181 P.3d at 326; *Pagan*, 165 P.3d at 730. For instance, in *Pagan*, 165 P.3d at 731, a division of this court explained that "even if the jury concluded that there was insufficient evidence to find beyond a reasonable doubt that [the] defendant stole property worth over $15,000, the trial court could still find by a preponderance of the

evidence that [the] defendant stole property worth over $15,000 for purposes of ordering restitution."

¶ 91 We agree with this rationale, and thus we decline defendants' invitation to reject the holdings of *Smith* and *Pagan*. Consequently, the jury's finding here that defendants' criminal acts caused less than $20,000 in loss did not preclude the trial court from finding that the prosecution established by a preponderance of evidence that defendants' criminal conduct caused loss greater than $20,000.

¶ 92 Defendants also argue that the trial court abused its discretion in awarding restitution based on what they claim were demonstrably false exhibits and testimony. Defendants point to Thomas Reed's testimony during the restitution hearing in which he admitted that some of the employee time shown in Exhibit 121 at trial as time spent on issues related to the crimes was not actually tied to defendants' criminal conduct. They also highlight sections of trial testimony in which defense counsel's cross-examination of Steven and Thomas Reed, Poole, and Benitez about time entered in Exhibit 121 showed that some of the time claimed might not have been time spent working on problems caused by the deletions. For

instance, defense counsel elicited testimony implying that Benitez was on vacation for some of the time that Exhibit 121 showed he was working, and Exhibit 121 showed Poole working for two days on issues related to the deletions that, according to Poole's trial testimony, were before he had been notified of the deletions.

¶ 93 Defendants further dispute Thomas Reed's testimony that all of the time entered on time sheets by Denver employees after the deletions under the category "2100" was time spent doing work related to the crimes. Defendants argue that this category in fact denoted all time spent at the office that was not billed against a specific job, not just time spent working on problems caused by the deletions. In support of this argument, defendants cite the time sheets admitted at the restitution hearing, which define category "2100" as "administrative/sales/shop/all other non-job related labor." They also emphasize Stotz's testimony at the hearing that when he was at EPS, the 2100 code was used generally to indicate "office overhead and administrative type work."

¶ 94 Finally, defendants argue that the trial court abused its discretion in failing to require EPS to apportion employee time expended to rectify problems caused by defendants' criminal

conduct from time required to fulfill routine and regular job responsibilities — time spent by successor employees taking over the jobs of the five employees who had resigned. Defendants point to Thomas Reed's cross-examination at the restitution hearing in which he agreed with defense counsel that his brother, Poole, and Benitez would have had to do some work in the weeks following the resignations that was unrelated to the deletions.

¶ 95 Regarding all these arguments, defendants essentially are asking us to make our own factual findings regarding the evidence. But it is the trial court's role, not ours, "to consider what weight should be given to all parts of the evidence, and to resolve conflicts, inconsistencies, and disputes in the evidence." *People v. Valdez*, 56 P.3d 1148, 1151 (Colo. App. 2002). We may not disturb the trial court's restitution award merely because some of the evidence might weigh against the amount awarded when other evidence supports the award.

¶ 96 For instance, Thomas Reed testified at the restitution hearing that the errors in the loss calculation presented at trial were corrected for the restitution hearing; that he "believed" or "assumed" that his brother, Benitez, and Poole did not use the code

2100 for time other than that spent on issues caused by the deletions; and that he thus believed that Exhibit 1 accurately showed the employee time spent working on such issues.

¶ 97 We reject defendants' contention that because Thomas Reed testified that he "assumed" or "believed" Exhibit 1 was accurate, the restitution order was supported only by "mere speculation." Exhibit 1 was based on his, Steven Reed's, Benitez's, and Poole's representations regarding how much time they spent working on issues caused by the deletions. The evidence at trial and at the restitution hearing provided sufficient proof that they spent the amount of time they claimed they did on such work.

¶ 98 Accordingly, the trial court did not abuse its discretion in the amount of restitution ordered.

IV. Conclusion

¶ 99 The judgments of conviction and the restitution orders are affirmed.

JUDGE RICHMAN and JUDGE DUNN concur.