Filed 10/25/13

CERTIFIED FOR PARTIAL PUBLICATION*

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

FIRST APPELLATE DISTRICT

DIVISION FOUR

THE PEOPLE, Plaintiff and Respondent, v. TERRY CHILDS, Defendant and Appellant.	A129583, A132199 (City & County of San Francisco Super. Ct. Nos. 207523, 2376395)

A jury convicted appellant Terry Childs of disrupting or denying computer services to an authorized user. (Pen. Code,[1] § 502, subd. (c)(5).) It also found true an enhancement allegation that damage caused by his offense exceeded $200,000. (§ 12022.6, subd. (a)(2).) He was sentenced to four years in state prison and ordered to pay more than $1.4 million in restitution. (§ 1202.4.) In two consolidated appeals from the conviction and the restitution order, he contends inter alia that subdivision (c)(5) of section 502 was not intended to apply to an employee.[2] We affirm the conviction and the restitution order.

* Pursuant to California Rules of Court, rules 8.1105(b) and 8.1110, this opinion is certified for publication with the exception of parts III through V.

[1] All statutory references are to the Penal Code unless otherwise indicated.

[2] Section 502, subdivision (c)(5) makes it a crime for any person who "[k]nowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network."

I. FACTS

A. *Employment Context*

From the time he was employed in April 2003 until July 2008, appellant Terry Childs served as the principal network engineer for Department of Telecommunications and Information Services (DTIS) of the City and County of San Francisco. DTIS was responsible for administering the city's computer network, providing computer services to city departments such as access to the Internet and to each department's database. It maintained the network, operated it, repaired it if it failed, and made any needed changes to it.

As part of the job application process, Childs was asked about his criminal history. On the first application, he reported that he had no prior convictions; on the second, he admitted that he had suffered one. In fact, Childs had been convicted of multiple criminal offenses in another state. Later, he admitted that he intentionally omitted giving accurate and complete criminal history information to the city at his hiring.

Childs worked at the city's data center at One Market Plaza in San Francisco. As DTIS's highest level engineer, he was highly knowledgeable, but he was also very sensitive and working with him could be difficult. Senior network engineer Glacier Ybanez assisted him. Childs reported to Herbert Tong, the manager of DTIS's network engineering unit. In February 2006, Richard Robinson became chief operating officer of DTIS and Tong's supervisor.

B. *The FiberWAN Network*

In 2005, Childs was assigned to configure, implement and administer the city's then-new fiber-optic wide area network—FiberWAN—using Cisco devices. He had lobbied to be allowed to implement the new network himself, rather than have Cisco do so. When he took on a project, he took ownership of it.

The FiberWAN network was set up side-by-side with the city's legacy computer system. When transfer from the legacy system was complete, FiberWAN could provide a single network infrastructure to most city departments, offering access to email, databases, encrypted information and the Internet. This single infrastructure operated at a

higher speed and for a lower cost than the legacy system. Information could be shared between departments or segregated to a specific department, as needed.

FiberWAN devices were both physically connected by cables and logically connected by the path along which data was transmitted between devices. Five core FiberWAN routers[3] were set up in three locations—two each at secondary sites and one at the One Market Plaza data center.[4] These key devices were linked so that an isolated disruption would not bring down the network. Instead, traffic was redirected through another router on the network. This design redundancy allowed the FiberWAN network to continue to operate while part of the network was being repaired, or if one device suffered a power failure. City departments had customer edge (CE) devices located at their sites. The DTIS routers and the city department CE devices were also linked to allow DTIS to provide computer services to each department.

As its principal network engineer, Childs developed the FiberWAN's configurations—the instructions needed to make the computer system work—based on standards set by the DTIS network architect. To protect the security of this critical infrastructure, all FiberWAN configurations were confidential.

Vital network information is usually stored in a computer system's non-volatile random access memory (NVRAM). Information "saved" to NVRAM can be accessed again if the computer is powered off and is then "rebooted." By contrast, information stored in volatile random access memory (VRAM) is lost once a computer is powered off and back on. If network configurations are stored in VRAM, they are lost when the system powers off and the system cannot reboot itself.

---

[3] A router is a device that chooses the best path to direct data.

[4] The data center had only one device because of DTIS budgetary constraints. DTIS's long-term plan was to acquire a second core router for the data center. In the meantime, the risk of failure of the single PE03 core router located at the data center was thought to be less than at the other two sites because the data center was staffed around-the-clock. Physical entry to the data center required multiple levels of electronic card reader approval.

Experts recommend that network configurations—or a backup copy of them[5]—be stored in NVRAM so that a power loss will not compel a complete reconfiguration of the network. To rebuild the configurations would cause a significant network disruption that might last for days. Likewise, network devices should not be run on VRAM, even if the security of the information in those devices is sensitive because the risk of losing that information in the event of a system crash is too great.

Childs had full administrative access to the FiberWAN computer system. Only a person with this access may make administrative changes to the network. Administrative access is essential in order to log into the network, to review network configurations, to troubleshoot problems, to add city departments, and to modify the network. To obtain administrative access to the network, a person must know the programmed password. Because network configurations are so vital to system administration, it is typical for several network engineers to have access to them.

Some FiberWAN computer devices have a password recovery feature that allows retrieval of backup configurations in case the primary configurations become corrupted. Password recovery is conducted through a device's console port. With physical access to a device through this console port—which is typically password-protected itself for security reasons—an administrator can access the network, clear out corrupted configurations and replace them with backup configurations, as long as the system can be rebooted. There is no way to reboot the network without powering off the computer and powering it back on again.

Configurations can also be restored by means of a modem connected to the network. A system administrator can access a network remotely to obtain what is called "out-of-band management" of the network—authorized access made by means outside the normal network flow. At two secondary computer sites, Childs installed devices that allowed him to dial into the computer network remotely if an emergency arose and he

[5] A backup copy of the configurations may be stored on a laptop computer. It appears that Childs used a laptop when he physically reloaded configurations onto core devices at a secondary DTIS site after a March 2008 fire.

was not able to be physically present at these locations. Such remote access by means of a dial-up modem poses a security risk, because it could permit undetected "back door" access by an *unauthorized* person. A record of the users entering the FiberWAN system was crucial to its integrity. Childs knew that when he used a modem to access core devices, no record of his use was tracked.

C. *Childs Assumes Sole Control of FiberWAN*

During the first months of work on the FiberWAN network, its configurations were available to all network engineers. Childs and his assistant Ybanez both had and used the password needed to access the FiberWAN. In 2006, the first city department was connected to FiberWAN, with other departments regularly added afterward.

Gradually, Childs became more possessive of the FiberWAN network. By July 2006, Robinson had received numerous complaints about network outages and service disruptions, some of which he believed were caused by undocumented FiberWAN changes. A memorandum went out to the network engineering staff, reminding them that all configurations changes were to be tracked, and noting that repeated failure to track changes could result in disciplinary action. Apparently, Childs regarded the memorandum as a personal attack on his authority. He responded by threatening to take a stress leave if DTIS outsourced any FiberWAN installations.[6]

In March or April 2007, Ybanez returned to the FiberWAN project after being on another assignment for many months. During that assignment, only Childs worked on FiberWAN. When Ybanez returned, he learned that the administrative access passwords had been changed and backup configurations had been moved off of a server once available to more of the network engineering staff.[7] Childs refused to give Ybanez administrative access to the FiberWAN, concerned that if pressed to do so, Ybanez would

[6] There was other evidence that Childs opposed outsourcing of any FiberWAN work, preferring to do it himself.

[7] Childs testified that Tong told him to take FiberWAN off this server, to prevent an unskilled person from modifying it.

reveal the access codes to management. Ybanez replied that he *would* tell management the access codes if asked, because the access codes did not belong to him.

From thereon, from the spring of 2007 on, only Childs had administrative access to FiberWAN. In May 2007, a city department had difficulty accessing a state database while Childs was away from DTIS without his cell phone or laptop—devices that would have allowed him to connect to the network from a remote location. When Tong instructed Ybanez to resolve the problem, Ybanez told Tong that he did not have administrative access to the network.

As Childs's supervisor, Tong was torn about his employee. Childs was an experienced and hard-working—albeit volatile—network engineer with a strong sense of responsibility for the network. Tong was under pressure to complete FiberWAN implementation, which Childs was working hard to accomplish. He hoped the implementation would be finished in another six to nine months. However, Tong knew that Childs's sole administrative access to FiberWAN made him the single point of failure, posing a danger to the city's computer network. The system could not function if Childs could not access it. Tong expected that eventually, Childs would give Ybanez access to FiberWAN. He also believed that Childs would not harm FiberWAN, as this would reflect badly on the principal network engineer's skill and expertise.

When Childs returned from vacation, Tong chose not to confront him about the limited access issue, fearing that Childs might retaliate by reducing his productivity. Instead, he hoped that the implementation would be completed soon and Childs would be reassigned to another project before the access issue became a problem. If DTIS did not have the FiberWAN password by that time, Tong believed that the password recovery feature would allow a new administrator to create a new one.

When Childs took extended time off, he delivered a sealed envelope to Tong that he said contained the FiberWAN passwords. Tong had no need for administrative access to FiberWAN during these absences. When Childs returned to work, Tong returned the unopened envelope to him to prove that he had not used them. Tong did not want Childs to speculate that someone modified the network configurations in his absence.

In December 2007, the city's Human Services Agency (HSA) experienced a power outage. When power was restored, its computers could not connect to FiberWAN—the configurations of its CE device had been erased because they had been saved to VRAM. Childs reloaded the configurations and got the system reconnected. When the HSA information security officer learned that the CE configurations had been stored in VRAM, he protested to Childs that this was unacceptable. Citing security concerns, Childs explained that he wanted to prevent a physical connection to the CE that would allow someone to obtain the configurations using the password recovery feature. He suggested disabling the password recovery feature instead; the information security officer agreed. Tong also agreed to this solution, as it would address a concern about hacking into the HSA's CE device. Soon, Childs disabled the password recovery feature on all CE devices citywide, and there were no backup configurations on any of the city's CE devices. As the password recovery feature could not be disabled on core PE devices, Childs erased their configurations that had been stored on NVRAM.

By the end of 2007, the city was planning how to connect the city's law enforcement functions on FiberWAN. The combined system would allow users access to state and federal databases. For security reasons, all DTIS employees had to pass a criminal background check in order to have access to the law enforcement system. Childs had adult felony convictions that he had not revealed when he applied to work for the city.[8] When asked to submit to a voluntary background check, Childs balked. Instead, he made a temporary arrangement with Tong and law enforcement officials to have Ybanez—who had passed his background check—escort him when Childs was

[8] In February 2005, a San Francisco County sheriff told Childs that he needed to undergo a criminal background check. Childs offered both his California and Kansas driver's licenses to the sheriff, prompting an out-of-state inquiry. The sheriff discussed his findings about Childs's criminal history with his supervisor, who agreed that Childs could work on the project. Months later, the sheriff acknowledged to Childs that he knew of this criminal history when he praised the network engineer for "turning his life around."

required to work on the law enforcement network. This procedure continued to be used through July 9, 2008.

In February 2008,[9] Ybanez was assigned to work on a police department network project that required him to have FiberWAN administrative access. Tong instructed Childs to give Ybanez administrative access to FiberWAN; Childs refused. When Ybanez asked what to do if FiberWAN went down and he was asked to support it, Childs responded that Ybanez was to call him.

Childs also told Ybanez that FiberWAN's password recovery feature was set up so that if Tong or other managers—whom he deemed to be unauthorized users—tried to reboot the system, it would erase the configurations, which were stored only in VRAM. Ybanez thought this was crazy; if there was a power failure, FiberWAN would cease to function, resulting in significant downtime. For his part, Tong knew that Childs had sought to run some configurations on VRAM. He instructed Childs not to do so because of the risk that the network would lose its configurations and because the practice inhibited password recovery. Tong did not know that Childs had placed *all* FiberWAN configurations in VRAM.

Tong instructed Childs to give *him* the FiberWAN passwords; again, Childs refused, fearing that Tong would pass it along to his manager. He opined that he was the only person capable of administering the network. He also cited another reason for his "refusal": because he had copyrighted the city-owned FiberWAN configurations as his own intellectual property.

By this time, Tong had a different view of the wisdom of Childs's sole access to the FiberWAN network. Initial implementation of FiberWAN to city departments was nearing completion, while Childs was becoming more uncooperative and unpredictable. At Tong's request, Cisco was asked for technical support about obtaining administrative access to FiberWAN.

[9] All dates refer to the 2008 calendar year unless otherwise indicated.

Tong also notified Robinson that a decision had to be made about their principal engineer. By then, Robinson knew that Childs had not passed his background check. He sought out more information about the engineer's criminal history. Reviewing the reports that Childs gave during the hiring process, Robinson saw the discrepancy between his initial job application reflecting no prior convictions and his time-of-hiring forms in which he admitted that he had once been convicted as an adult. Tong believed that Childs had suffered a juvenile conviction, but Robinson learned that Childs had been convicted of a criminal offense as an adult. The adult conviction and the perjured filing of personnel records were both grounds for dismissal.

Meanwhile, in March 2008, a fire at the Department of Public Works resulted in a power loss at secondary DTIS sites. Both core routers went down, but traffic was taken up by other core routers. In the past, Childs had asked DTIS to purchase terminal servers for both secondary DTIS sites. Those requests were denied on the ground that these additional devices were unnecessary and insecure. After the fire, Childs installed his own terminal servers at these locations. He also connected modems and telephone lines to these servers. Together, these links allowed him to have "out-of-band" management of those core devices, so that remotely, he could restore the configurations from another location—even from his home. This connection also allowed him to enter the FiberWAN system undetected. The terminal servers were password-protected; only Childs knew those passwords. In the One Market Plaza main data center, Childs often worked in a locked laboratory. No one else worked in the laboratory unless he was present.

By March, Childs had intentionally configured the core FiberWAN devices so that if a power outage occurred, the configurations stored in VRAM would be lost and these core devices would be offline until he physically uploaded a backup configuration. If the configurations had been stored to NVRAM instead, they would have automatically reloaded onto the devices shortly after power was restored. The same result would occur if someone attempted a password recovery or if an unauthorized user attempted to enter the system.

By May, DTIS employees had been notified about the possibility of layoffs. Childs was unconcerned. "They can't screw with me," he told a coworker. "I have the keys to the kingdom."[10]

D. *Workplace Violence Concerns Arise*

In June, concerns about Childs's conduct came to a head. DTIS was moving its One Market Plaza data center to a new location. Its new security manager—Jeana Pieralde—sought to inventory FiberWAN's devices at the data center in preparation for the move. This inventory required a computer scan of the network in order to generate a report of what devices were on the network and their configurations. If a computer was turned off, she had to turn it on in order to complete the scan. In the late afternoon on Friday, June 20, Pieralde came to the data center to conduct the inventory, having obtained keys to enter any locked areas.

Childs had not been notified of Pieralde's plan to conduct this inventory. He was very upset by her presence, ranting at her in an agitated manner. He confronted her, taking photographs of her with his cell phone. Concerned by his aggressive response, Pieralde locked herself inside an office and called Robinson to report this incident. At least one DTIS staffer left the site, fearing the potential for violence.

Childs called Tong to complain about Pieralde. When Tong did not share his concern, Childs said angrily "This means war and I am ready." Later, Tong reported this statement to police. Childs also called the city's chief information officer to complain.

In response to Pieralde's complaint, Robinson made his own call to Childs. He told him to stop interfering with her work. Childs challenged Robinson's authority to conduct an inventory, accusing him of creating a hostile work environment. Angrily, he said: " 'I know what you are up to. I am ready for you.' " In a loud and combative tone, he threatened to come to Robinson's office. Robinson ordered Childs to leave the data center and said that he would revisit the issue on Monday.

[10] Childs admitted saying this, but said that this was a joking reference to his superior skill level.

This incident left DTIS management concerned about Childs's potential for workplace violence. In the next few weeks, the issue was discussed at several meetings. Robinson talked about this with his supervisor, with representatives of the city's Human Resources (HR) Department, and the city attorney's office and—because of his employee safety concerns—with police.[11]

At this point, Robinson learned that Childs was the only person with administrative access to FiberWAN. He consulted Cisco officials about ways to allow the city to recover control of the network.

Meanwhile, an HR representative sought to meet with Childs about this matter. He did not respond to her requests until July 3, when he indicated that *his* issues had been resolved. On July 7, the HR representative replied that concerns raised by *other employees* still needed to be addressed.

In early July, it was decided that Childs was to be reassigned. At July 7 and July 8 meetings, representatives of DTIS, HR, the city attorney's office, and the police department discussed about how best to obtain administrative access from Childs. A union representative was advised of a planned July 9 meeting at which Childs would be informed of the reassignment. The representative was advised that the meeting would not be a disciplinary matter, but that it could become one if Childs refused to disclose the user ID and password. The union representative declined to participate in the planned July 9 meeting, concluding that DTIS had a right to know this information.

E. *Reassignment*

On July 9, Childs and Ybanez went to the Hall of Justice's data center to connect the police department's computer system to FiberWAN. Childs used the city laptop he removed from his backpack to do some of this work. A coworker called him on his cell telephone to tell him that he would be reassigned and removed as the FiberWAN network engineer. Soon, the police department's acting chief information officer escorted him to another room for a meeting. Childs brought the laptop and his backpack with him.

[11] Pieralde had also filed a police report about the incident.

Robinson and an HR representative were waiting for Childs. A speaker phone[12] was connected to the DTIS data center, where Tong, DTIS workers and Cisco personnel listened in. They could test whether the passwords Childs might provide would allow DTIS to obtain administrative access to the system.

Robinson told Childs that he was being reassigned. He asked Childs for user IDs and passwords to FiberWAN's core devices. At first, Childs said that he no longer had administrative access to FiberWAN; Robinson knew this was untrue.[13] Later, Childs knowingly provided incorrect passwords that did not allow access to FiberWAN. He also told Robinson that DTIS management was not qualified to have the FiberWAN user IDs and passwords.[14] When asked for backup configurations, Childs said that there were none.[15] Robinson ordered Childs to reveal them, to no avail.

After 40 to 60 minutes, San Francisco Police Inspector James Ramsey joined the meeting. He advised Childs that his failure to cooperate could be a violation of Penal Code section 502.[16] Childs made no response to this statement. Ramsey pleaded with him for cooperation, but he was not able to obtain the desired information from Childs, either.[17]

---

[12] Three experts testified that it was unwise to give an administrative password and user ID over a speaker phone.

[13] Childs later admitted that he had changed the password on the morning of the meeting.

[14] A defense expert testified that it was not a best practice to give management access to network devices. Generally, management does not require administrative access to its computer network.

[15] At trial, Childs admitted that this was untrue.

[16] Ramsey did not advise Childs of his *Miranda* rights at any time during this July 9 meeting.

[17] At one point during this meeting, Childs asked for an ambulance, saying that he did not feel well. He later testified that he experienced chest pains, but witnesses testified that his demeanor did not change noticeably before he made this request. He was offered an ambulance but later declined that offer. He admitted that he never consulted a doctor after these pains arose.

It became apparent to Robinson that Childs would not provide FiberWAN access. Childs was placed on administrative leave for failure to do so. Robinson accepted Childs's city identification, keys, pager, and cell telephone, but the engineer did not offer the city-owned laptop that was inside his backpack. Childs left the meeting with Ramsey.[18] After receiving a receipt for the city property he relinquished, Childs left the building.

Childs later admitted that when he was at the meeting, he had the FiberWAN access codes and a backup of its configurations on a DVD in his city-owned laptop inside his backpack.[19] With this DVD—which was itself password-protected and encrypted—and his laptop, Childs could have remotely connected with the network if he had Internet access.

F. *July 9-July 21 Events*

Back at the data center, DTIS staff searched Childs's workspace and locked laboratory looking for FiberWAN configurations. In his laboratory, they were surprised to find two filing cabinets, each secured by a cabinet lock and two padlocks. Each cabinet had a hole manually cut out of the side, through which cables had been fed leading to a computer device. These active devices could permit someone without physical access to the data center to access the FiberWAN network. The possibility that Childs might have undetected remote access to FiberWAN heightened security concerns and led to a more intensive response than merely recovering administrative access.[20] The devices were physically disconnected from the network but were left running. By July 11, new devices monitored any unauthorized FiberWAN intrusions.

---

[18] About this time, Ramsey also gave Childs a written copy of section 502. He testified that he recalled making specific mention of violating subdivision (c)(5).

[19] Childs testified that he always had these backup configurations with him.

[20] On July 10, Childs contacted police to say that he would not attempt to access FiberWAN.

DTIS had no administrative access to the FiberWAN network. Outside consultants and DTIS employees began intensive efforts to recover control of the FiberWAN network. No configurations could be found.

Meanwhile, on July 10, Childs received a letter advising him that he had been placed on paid administrative leave until an administrative hearing planned for July 14 would be conducted. If it was determined that he had refused to give DTIS management access to FiberWAN, his administrative leave would then be unpaid.[21] He contacted HR and arranged to have the review hearing postponed to July 18. Childs also asked police for return of his terminal servers located at the two secondary DTIS sites.

Childs drove to Nevada, taking his city-owned laptop and the backup configurations with him. Needing money and an attorney to assist him at the July 18 administrative review hearing, he withdrew almost $10,000 from his bank account on July 11 and 12. This left less than $200 in his account. On his return to his Pittsburg home on the night of July 12, he was arrested. He had more than $10,000 on his person at that time. This money was seized. Questioned after his arrest, Childs invoked his privilege against self-incrimination.

At first, DTIS efforts focused on obtaining FiberWAN access without interrupting city computer service. Once DTIS's lack of administrative access to its computer network became publicly known, pressure increased to restore that access. By July 17, it became clear that non-disruptive efforts would not soon succeed and efforts to recover access became more aggressive, even at the risk of disrupting ongoing computer service to city departments.

Before his suspension, Childs knew that a July 19 power outage was scheduled at the data center, to allow maintenance work to be done on the building's main power supply. Technicians realized that losing network power before first regaining administrative control of FiberWAN risked the loss of the configurations, which could severely disrupt city computer services. DTIS postponed the planned power outage.

[21] Ultimately, Childs would be suspended without pay.

On July 21, Childs—through his attorney—gave the correct FiberWAN passwords and backup configurations to then-Mayor Gavin Newsom.[22] After an initial attempt at access failed, Childs provided additional information that allowed DTIS to regain administrative access to FiberWAN through a specific device.

During the period from July 9 through July 21, DTIS was effectively locked out of the FiberWAN network. Neither DTIS employees nor other computer experts were able to obtain administrative access to the network until Childs revealed the access codes. There were no network service outages, but in the next two weeks, neither DTIS employees nor computer experts hired by the City were able to access the network in order to administer it. They could not diagnose problems, maintain the network, review or change its configurations, or update it to serve the more than 65 city departments then on the network. In addition to postponing the power outage, plans to add two city departments to the network in mid-July had to be postponed. The city was unable to add new city departments to FiberWAN, nor could it remove Childs as system administrator and appoint a new one.

Within days of the city's recovery of administrative access to FiberWAN, the network became a team project. By the time of trial, a new principal engineer and other network engineers had administrative access to FiberWAN. A backup copy of the configurations was again stored on a server that could be accessed by several DTIS engineers. Network recovery work continued through late November. The city paid outside consultants $646,000 for evaluation of FiberWAN. DTIS staff time spent to regain access to FiberWAN was worth $220,000. An expert testified that if administrative access had not been recovered, rebuilding the FiberWAN configurations would have cost the city $300,000.

G. *Charges and Pretrial Matters*

In mid-July, Childs was charged with one count of disrupting and denying the use of the city's computer network. He was also charged with three counts of illegally

[22] Childs testified that because the access issue had become public knowledge, he wanted to provide FiberWAN access in a manner that could be proven.

providing access to the network through the modems. The complaint alleged an enhancement based on the loss of property worth more than $200,000. (§§ 502, subd. (c)(5)-(6), 12022.6, subd. (a)(2).) He was held on $5 million bail. Childs pled not guilty and was held to answer on all charges after a preliminary hearing. His motion to suppress evidence of his July 9 statements was denied in December.

In January 2009, an information was filed charging Childs with the same four offenses and the one enhancement. (§§ 502, subd. (c)(5)-(6), 12022.6, subd. (a)(2).)[23] Later that month, Childs demurred to the three modem counts and renewed his motion to suppress evidence obtained as a result of his July 9 statement, without success.

Childs also moved to set aside the information on the ground, inter alia, that there was insufficient evidence to support the charges. (§ 995.) The prosecution opposed the motion. In August 2009, after hearing, the trial court dismissed the three modem counts.[24]

H. *Trial and Sentencing*

1. *Prosecution Case*

Childs was tried on the remaining charge of disrupting or denying computer services to an authorized user. The prosecution's theory of the case was that Childs acted as if he—not the city—owned the FiberWAN network and that he believed that his sole

[23] Sections 502 and 12022.6 have been amended since July 2008. (See former §§ 502, subds. (c)(5), (6), (h)(1) [Stats. 2000, ch. 635, § 2, pp. 4147-4149]; 12022.6, subd. (a)(2) [Stats. 2007, ch. 420, § 1, p.3675].) As the current versions of these subdivisions are identical to those in effect on the date of the offense, we do not make repeated references to the 2008 versions of the statutes that we apply. (See §§ 502, subd. (c)(5), (6), (h)(1) [Stats. 2011, ch. 15, § 378]; 12022.6, subd. (a)(2) [Stats. 2010, ch. 711, § 5].)

[24] Each side challenged aspects of this ruling by writ petition. We denied both petitions in October 2009. The People also appealed this order, but after Childs was convicted of the remaining charge, the appeal was abandoned and we dismissed it on the People's request. At Childs's request, we took judicial notice of the record in this earlier appeal in 2011, without making an initial determination of relevance. As this record contains crucial documents that we did not find in our record on appeal, we now find the prior record to be relevant to our determination of the issues in the current appeal.

access to the computer system gave him job security. It put on evidence that by preventing anyone else from having administrative access to the FiberWAN network, Childs sought to keep from being laid off or from having his work outsourced. He knew he could not pass a criminal background check that threatened to force his removal from the FiberWAN work. He also developed means to have undetected access to the network.

Much of the six-month trial was devoted to understanding the technical capabilities of the FiberWAN network and the manner in which Childs modified them. The prosecution put on evidence that by failing to reveal his administrative password, Childs deprived the city of part of its network. By locking the city out of the FiberWAN network, he disrupted the city's computer services. Besides the evidence of sole administrative control and running the FiberWAN configurations on non-stored VRAM, the jury heard other evidence of Childs's conduct:

Disabling Console Ports. The jury learned that if the console port—the physical means of access to the network on the device itself—is disabled, then the administrator cannot login to the system using what is regarded as the "port of last resort." On July 8—the day before he was placed on administrative leave—Childs disabled the console ports on all five core devices, preventing the possibility of any password recovery.

Applying Access Controls. Childs also applied access controls to core devices that required that all administrative access had to be achieved by means of one particular computer, even if the access codes were known. He set up these access controls on core devices on the morning of July 9.[25] After regaining control of FiberWAN on July 21, DTIS learned that all CE devices also had these access controls applied to them. All FiberWAN core devices had been set up to inform the network administrator if anyone other than Childs tried to logon to one of them and from what specific location the attempt was being made. According to a prosecution expert, that information could allow the administrator to deny DTIS access to the network merely by changing the password.

[25] Childs testified that he did this because he knew he would be working at the Hall of Justice that day and wanted FiberWAN access while he was there.

Filing Copyright Documents. In July 2007, Childs applied to copyright a slightly sanitized version of city's FiberWAN design and configurations as his own intellectual property. In January 2008, he filed an updated submission. He did so despite having acknowledged that these configurations were the city's intellectual property and were protected from disclosure by federal Homeland Security considerations. The design and configurations that Childs provided with his application showed the physical locations of some network devices that were not publicly known. That information was deposited with the Library of Congress where it was available for public inspection.[26] The publication of this confidential information made the FiberWAN network more vulnerable to intrusion.

The jury heard expert testimony that DTIS had no administrative access to FiberWAN if the sole person with administrative access refused to give network management access to network devices, the configurations were not on the device, backup configurations were unavailable, the console port has been password-protected and the devices were run on VRAM. If power to the system was lost, the configurations would be wiped out and would need to be completely rebuilt, denying access to the computer system for a significant time. In the view of prosecution witnesses, Childs's refusal to reveal the access codes caused a denial of services because DTIS was unable to add new city departments to FiberWAN.

Childs made himself to be a single point of failure for the FiberWAN network, creating the possibility that the network could collapse without him in a system that was intended to have backups and redundancy to prevent disruption of the network. Prosecution witnesses told the jury that it was in the city's best interest to have more than one person with administrative access to FiberWAN in case one person was unavailable. DTIS's inability to access its network meant that something within FiberWAN was "radically wrong," posing a very difficult problem to resolve. It was also unusual—less than 1/10th of 1 percent of all Cisco networks worldwide required the kind of

[26] Childs testified that he was unaware that the documents would be available to the public.

intervention that FiberWAN did. At the close of the prosecution's case-in-chief, Childs's moved for acquittal without success. (§ 1118.1.)

2. *Defense*

Childs testified in his own defense. He admitted much of the conduct that formed the basis of the prosecution. He admitted that he had exclusive administrative access to the FiberWAN network, that he lied to his managers when he said that he did not, and that he sought to copyright its configurations. On July 9, the network was encrypted with a password that only he knew. He had control of the backup configurations, which were not available to DTIS and which had been encrypted. He had disabled the password recovery feature on the CE devices and had disabled the console ports on all devices. He admitted that he ran FiberWAN core devices on VRAM. If an engineer attempted a password recovery of a core device, he knew that the device would shut down, and when it was rebooted, it would be blank.

Childs testified that he acted as he did to protect the security of the FiberWAN network. He believed that DTIS management was too lax about network security.

The prosecution put on evidence to undermine this defense. It noted the risk to the city from his copyright application, which Childs admitted filing. He had failed to cite network security reasons for his decisions at the time that he made them. He did not mention security concerns on July 9 when he refused to reveal the FiberWAN password and user ID. Instead, he refused to give Robinson FiberWAN access because he did not believe that Robinson was authorized to have administrative access to the network.

3. *Argument and Verdict*

The prosecution reasoned that Childs's conduct had damaged the city in several ways. He made the network vulnerable to intrusion; he precluded DTIS from maintaining, troubleshooting or adding new city departments onto the network; and he required the city to spend large sums of money to regain administrative access to its network.

For his part, Childs urged the jury to conclude that his dispute with the city was an employment matter, not a criminal act. He claimed that he acted within the scope of his employment, a defense to the charge. (See § 502, subd. (h)(1).)

He also argued that he did not knowingly disrupt or deny computer services to an authorized user because other DTIS officials such as Robinson lacked the skills needed to implement the FiberWAN network. Childs argued that after he was reassigned, no one at DTIS was a qualified user. The city brought the problem on itself by threatening him after the June 20 incident, by ambushing him at the July 9 meeting, and by failing to respect his professional stature. Childs claimed that his conduct was reasonably necessary to protect the FiberWAN network from unauthorized intrusion because no one else at DTIS was competent to administer it.

Childs also disputed having denied computer services to the city because FiberWAN continued to operate during the July 9-21 period. He reasoned that no harm was done. He did not believe that he denied or disrupted computer services; if he was mistaken, he argued that his reasonable mistake negated the required criminal intent to find him guilty of violating subdivision (c)(5) of section 502.

The jury found Childs guilty of the charge and found the enhancement allegation to be true. (§§ 502, subd. (c)(5), 12022.6, subd. (a)(2).) His motion for arrest of judgment was denied, as was his motion for new trial.

In August 2010, Childs was sentenced to four years in state prison—a midterm of two years for the offense and a two-year consecutive enhancement term for excessive taking. Based on his prior convictions, the trial court rejected his claim for additional presentence conduct credit.[27] The issue of restitution was reserved.

[27] Childs challenged this presentence credit determination in his opening brief, but—as he has already completed his prison term and his rights are no longer affected—he concedes that the issue is moot. (See *DeFunis v. Odegaard* (1974) 416 U.S. 312, 316; *Keefer v. Keefer* (1939) 31 Cal.App.2d 335, 337; see also 9 Witkin, Cal. Procedure (2008) Appeal, § 326, p. 375.)

In May 2011, Childs was ordered to pay $1,485,791 in restitution to DTIS.[28] His motion for return of $10,744[29] seized from him at the time of his arrest was denied and that sum was applied toward the amount of restitution owed.[30]

II. HACKING

A. *Employment Dispute*

Several challenges that Childs raises to his conviction turn on a single argument: that subdivision (c)(5) of section 502 was meant to apply only to unauthorized computer users—hackers—and not to an employee who was authorized to use the computer system but did so in a manner that vexed the employer. (See pts. III.A.2, III.C.1.b.i, III.C.2, III.E., IV.B, *post.*) He asserts that his acts fell within the scope of employment defense set out in subdivision (h)(1) as a matter of law. As this underlying issue is pivotal to so many interrelated question, we address it first.

When analyzing statutory language, we are charged to examine the language itself, the legislative history of the provision and case law construing the crucial language, in that order. (*People v. Heitzman* (1994) 9 Cal.4th 189, 200; see *In re Noreen G.* (2010) 181 Cal.App.4th 1359, 1375.) We conduct those inquiries below.

B. *Evolution of Offense*

Childs reasons that the charged offense is inapplicable to him as a matter of law because no employee has yet been convicted for refusing to reveal a computer user name and password to an employer on demand. The correct inquiry is not whether an employee has ever been convicted of the charged offense on the basis of similar conduct in the past, but whether the legislature intended to hold criminally liable one who acted as Childs did.

---

[28] The City Attorney's separate request for $32,933.71 in restitution was denied.

[29] The record suggests some confusion about whether this amount was $10,744 or $10,774. We assume that $10,744—the amount ordered to be credited against Childs's restitution order—is correct.

[30] In this consolidated appeal, we have considered the records in both of these pending appeals. Thus, we need not also take judicial notice of the record on appeal from his conviction in the appeal of the restitution order, as Childs requested.

To determine the legislative intent, we first review the evolution of section 502. There have been many revisions to state law banning computer crimes since a predecessor statute was first enacted in 1979.[31] That provision made two types of computer use criminal—accessing a computer system to commit fraud or theft; and accessing, altering, deleting, damaging or destroying a computer system. (See Stats. 1979, ch. 858, § 1, pp. 2968-2969 [adding prior version of § 502].) In 1985, the prior version of section 502 added a third computer offense—unauthorized accessing of a computer—and amended another offense to ban the malicious destruction or disruption of a computer system. (See Stats. 1985, ch. 571, § 1, pp. 2076-2077.) In all of these early versions of computer crimes, accessing the computer system was a key element of the offense.

In 1987, when the prior statute was repealed and a new version of section 502 was added, the law set out seven distinct computer offenses. One made the knowing and unpermitted disruption or denial of computer services a public offense—the same offense with which Childs was later charged. (See Stats. 1987, ch. 1499, §§ 2-3, pp. 5782-5786.) Two more offenses—introducing a contaminant into a computer system and using another's Internet domain name to send damaging email messages—were added in 1989 and 1998, which brings the total of computer crimes to nine. (See Stats. 1998, ch. 863, § 3, pp. 5484-5488; Stats. 1989, ch. 1357, §§ 1.3, pp. 5736-5740.) In 2008 at the time of the offense charged against Childs, some of the nine computer offenses specifically required unpermitted access as an element. (See § 502, subd. (c)(5); compare § 502, subds. (c)(1)-(2), (4), (7) [access]; see also § 502, subds. (c)(3) [use], (6) [providing access].) Some did not—the charge against Childs among them. (See § 502, subds. (c)(5) [disruption], (8), [contamination], (9) [sending false email].)

[31] Section 502 has been enacted, amended, repealed, added anew, and amended again—both before and since the date of the 2008 charged crime. For convenience, we refer to the predecessor statute as "prior section 502," and the statute in effect at the time of the offense as "new section 502."

In 1987, section 502 explained the purpose of the statute. By its express terms, the Legislature intended "to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. [The] proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data. [¶] [The] protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data." This statement of legislative intent was unchanged in 2008, when Childs allegedly violated subdivision (c)(5). (§ 502, subd. (a) [Stats. 2000, ch. 635, § 2, pp. 4144-4145]; see Stats. 1987, ch. 1499, §§ 2-3, pp. 5782-5783.)

C. *Evolution of Defense*

The prior statute enacted in 1979 was silent on the applicability of the computer crimes statute in an employment context. (See Stats. 1979, ch. 858, § 1, pp. 2968-2969.) By 1985, *one* of the three computer offenses then codified—unauthorized computer access—specifically provided that it did not apply to one who accessed an employer's computer within the scope of employment. (See prior § 502, subd. (d) [Stats. 1985, ch. 571, § 1, pp. 2076-2077].) The 1987 enactment of the new statute set out an employment defense applicable to *all* section 502 offenses if an employee acted within the scope of his or her lawful employment.[32] (See § 502, subd. (i)(1) [Stats. 1987, ch. 1499, §§ 2-3, pp. 5782-5786]; now § 502, subd. (h)(1).) In 1999, the Legislature first defined the scope of employment defense. "For purposes of this section, a person acts within the scope of his or her employment when he or she performs acts which are

[32] The statute also provided a defense for employees acting outside the scope of employment, but that defense is not at issue in the case before us. (See § 502, subd. (h)(2).)

reasonably necessary to the performance of his or her work assignment." (See § 502, subd. (h)(1) [amended Stats. 1999, ch. 254, § 3, p. 2292].) The same statutory language was in effect in 2008, when Childs was charged with the current offense. (See § 502, subd. (h)(1) [Stats. 2000, ch. 635, § 2, pp. 4144-4150].)

D. *Statutory Construction*

1. *Subdivision (c)(5) Offense*

Childs contends that the language of subdivision (c)(5) must be read in light of the legislative purpose set out in subdivision (a) stating that the law was intended to protect against unauthorized access to computer systems. He reasons that subdivision (c)(5)—which contains no express requirement of access—must be read to imply one in order to be consistent with the legislative intent behind section 502.

This claim of error requires us to apply basic rules of statutory construction. The interpretation of a statute and its applicability pose questions of law for us to determine on appeal. (*People v. Cole* (2006) 38 Cal.4th 964, 988; *Estate of Madison* (1945) 26 Cal.2d 453, 456.) The overriding goal of statutory construction is to ascertain the legislative intent behind the statute, in order to give effect to that intent. (*People v. Mejia* (2012) 211 Cal.App.4th 586, 611.) In this analysis, the text of the statute is the best indicator of legislative intent. (*Tonya M. v. Superior Court* (2007) 42 Cal.4th 836, 844; *People v. Johnson* (2006) 38 Cal.4th 717, 723-724.) When interpreting statutes, we begin with the plain, commonsense meaning of the language that the Legislature used. If that language is unambiguous, then the plain meaning of the statute controls. (*People v. Mejia, supra,* 211 Cal.App.4th at p. 611; *Surfrider Foundation v. California Regional Water Quality Control Bd.* (2012) 211 Cal.App.4th 557, 575.)

On its face, subdivision (c)(5) is unambiguous. (See, e.g., *People v. Albillar* (2010) 51 Cal.4th 47, 55.) Its plain meaning seems to be that Childs—who was given authorized access to the FiberWAN network—may be convicted under its terms. However, he contends that subdivision (c)(5) contains a latent ambiguity when read together with the "unauthorized access" language in subdivision (a) in the statement of legislative purpose behind section 502. A latent ambiguity exists when a literal

interpretation of a statute would frustrate the purpose of the statute. (*Varshock v. Department of Forestry & Fire Protection* (2011) 194 Cal.App.4th 635, 644.) When faced with a latent ambiguity, we must determine which interpretation of the statute is most consistent with the legislative intent. We infer that the Legislature intended an interpretation producing practical, workable results, not one producing mischief or absurdity. (*Gattuso v. Harte-Hanks Shoppers, Inc.* (2007) 42 Cal.4th 554, 567.)

For many reasons, we reject Childs's claim that the Legislature intended that unauthorized access is an implied element of subdivision (c)(5). We find his focus on the "unauthorized access" language of subdivision (a) to be too narrow. When determining legislative intent, our analysis does not turn on a single word or phrase. We must construe the language in the context of the statute as a whole, giving meaning to every part of it. (*Tonya M. v. Superior Court, supra,* 42 Cal.4th at p. 844; *People v. Zeigler* (2012) 211 Cal.App.4th 638, 650.) Subdivision (a) sets out a series of evils deserving of protection, of which unauthorized computer access is one. The Legislature expressly stated its intent to protect against "tampering, interference, damage, and unauthorized access" to computers. (§ 502, subd. (a).) Disrupting or denying computer services to an authorized user could reasonably be read to fall within "interference" with computers, even without a showing of unauthorized access.

Childs's related argument—that the reference in subdivision (a) to the need to combat "computer crime and other forms of unauthorized access" to computers requires us to read an unauthorized access element into all subdivision (c) offenses—is somewhat more plausible. However, as we shall explain, other principles of statutory construction lead us to reject this argument, too.

Significantly, Childs's interpretation of section 502 fails to acknowledge differences among the wording of subdivision (c) offenses. Four of the section 502, subdivision (c) offenses include access as an element. (See § 502, subds. (c)(1)-(2), (4), (7).) The provision under which Childs was charged does not. (See § 502, subd. (c)(5).) When different words are used in adjoining subdivisions of a statute that were enacted at the same time, that fact raises a compelling inference that a different meaning was

intended. (*People v. Albillar, supra,* 51 Cal.4th at p. 56; *Metropolitan Water Dist. v. Superior Court* (2004) 32 Cal.4th 491, 502; *Yao v. Superior Court* (2002) 104 Cal.App.4th 327, 333.) The Legislature's requirement of unpermitted access in some section 502 offenses and its failure to require that element in other parts of the same statute raise a strong inference that the subdivisions that do not require unpermitted access were intended to apply to persons who gain lawful access to a computer but then abuse that access. (See *Arden Carmichael, Inc. v. County of Sacramento* (2001) 93 Cal.App.4th 507, 516 [every word excluded from a statute is presumed to have been excluded for a reason].)

2. *Subdivision (h)(1) Defense*

We are also persuaded the Legislature did not intend to imply an access element into every subdivision (c) offense because the legislative history of the employment defense codified in subdivision (h)(1) is inconsistent with this reading of subdivision (c). The unlawful access of an external hacker is inherently inconsistent with the permitted access of an employee, making the scope of employment defense relevant to this issue. When statutory language is ambiguous, we may consult extrinsic aids such as legislative history to help us interpret the statute. (*People v. Cole, supra,* 38 Cal.4th at p. 975; *People v. Mejia, supra,* 211 Cal.App.4th at p. 611; see *People v. Rodriguez* (2002) 28 Cal.4th 543, 549-550.)

When the Legislature defined the "scope of employment" defense in 1999, this was intended to "[close] a loophole that allows disaffected employees to maliciously tamper with a company's database" and to discourage "a malicious employee's victimization of an employer." (See Assem. Com. on Public Safety, Rep. on Assem. Bill 451 (1999-2000 Reg. Sess.) Apr. 6, 1999, p. 6; Sen. Com. on Public Safety, Rep. on Assem. Bill 451 (1999-2000 Reg. Sess.) June 22, 1999, p. 9 [same].) These legislative sources make clear that one effect of the 1999 amendments to the employment defense now set out in subdivision (h)(1) was to broaden its application beyond external hacking and to encompass employee misconduct. Since the amendments took effect in 2000, the scope of employment defense no longer shield employees from prosecution for acts that

were not reasonably necessary to the performance of the employee's work assignment. (See § 502, subd. (h)(1).) This conclusion is also supported by the legislature's 2000 expansion of the definition of "injury" to a computer network to include the denial of access to a legitimate user. (§ 502, subd. (b)(8) [Stats. 2000, ch. 635, § 2, pp. 4144-4150].)

3. *Subdivision (e)(1) Remedies*

Childs also argues that the 2000 amendment of the scope of employment defense in subdivision (e)(1) supports his conclusion that section 502 was not intended to punish any employee. In fact, the legislative history supports a contrary view. At one time, subdivision (e) of section 502 required that a criminal conviction be obtained *before* a victim of computer crime could seek the civil remedy provided in that provision. In 2000, the Legislature amended section 502 to allow a private civil action "regardless of whether a criminal conviction has been obtained." (Sen. Rules Com., Off. of Sen. Floor Analyses, 3d reading analysis of Assem. Bill 2727 (1999-2000 Reg. Sess.) as amended August 25, 2000, p. 5.) If section 502 banned Childs's conduct, the statutory language is clear that the prosecution had lawful authority to charge him with a criminal offense, regardless of whether his actions could also constitute the insubordinate employee conduct.

In a related argument, Childs reasons that his conduct was merely insubordinate and should have been resolved by civil means as an employment dispute, rather than by a criminal prosecution. (See § 502, subd. (e).) His reasoning is unpersuasive. It assumes wrongly that if a civil action is proper, insubordinate employee behavior can never be so grievous that it might also justify the filing of criminal charges. It also fails to appreciate the role of the separation of powers in this issue. The prosecution—as part of the executive branch of our government—ordinarily has sole discretion to conduct criminal cases, including determinations of whom to charge and what charges to file. (*Manduley v. Superior Court* (2002) 27 Cal.4th 537, 552; *Dix v. Superior Court* (1991) 53 Cal.3d 442, 451; *Gananian v. Wagstaffe* (2011) 199 Cal.App.4th 1532, 1540.) A prosecutor's decision about filing criminal charges arises from complex law enforcement

considerations that are not generally subject to judicial supervision. (*Manduley v. Superior Court*, *supra*, 27 Cal.4th at p. 552.)

4. *Conclusion*

These principles of statutory construction combine to convince us that the Legislature did not intend that subdivision (c)(5) could only be applied to external hackers who obtain unauthorized access to a computer system. It appears that subdivision (c)(5) may properly be applied to an employee who uses his or her authorized access to a computer system to disrupt or deny computer services to another lawful user.

E. *Analysis of Case Law*

Despite the statutory language, Childs asserts that case law lends support to his claim that subdivision (c)(5) was not intended to apply to an employee as a matter of law. Case law is significant to statutory construction because once a statute is construed by the courts, we presume that the Legislature is aware of that construction. If the Legislature does not alter that construction by subsequent legislation, we presume that it approved of the judicial construction. (*People v. Hallner* (1954) 43 Cal.2d 715, 719.) We have conducted a careful review of the cases that Childs cites, but none of them persuade us that subdivision (c)(5) may not lawfully be applied to an employee who misuses the grant of authorized access he was given to his employer's computer system. We conclude that each case is distinguishable from the situation before us in a significant manner.

In *Mahru v. Superior Court* (1987) 191 Cal.App.3d 545, an employee—acting at the behest of his employer—took steps to ensure that a third party user of the employer's computer system could not use it any longer. The employee was charged with maliciously altering a computer system under a statutory predecessor to section 502. (See Stats. 1979, ch. 858, § 1, pp. 2968-2969 [adding prior version of § 502]; Stats. 1985, ch. 571, § 1, pp. 2076-2077 [subd. (c) as charged in *Mahru*], Stats. 1987, ch. 1499, §§ 2-3, pp. 5782-5786 [repealing prior version and adding current version of § 502].) The term "maliciously" is defined as a wish to vex, annoy or injure a third party. (§ 7, subd. 4.) The appellate court ruled that the predecessor statute did not apply, because the computer system allegedly altered was not owned by the third party, but by the employer.

(*Mahru v. Superior Court, supra,* 191 Cal.App.3d at pp. 548-549; see *Facebook, Inc. v. Power Ventures, Inc.* (N.D. Cal. July 20, 2010, No. C08-05780) 2010 WL 3291750, p. 8.)[33] This case is clearly distinguishable from the one before us. Unlike *Mahru*, Childs acted against his employer's wishes in a manner affecting the employer's computer system.

In dicta, the *Mahru* court went on to assert its view that the Legislature "could not have meant, by enacting section 502, to bring the Penal Code into the computer age by making annoying or spiteful acts criminal offenses whenever a computer is used to accomplish them. Individuals and organizations use computers for typing and other routine tasks in the course of their affairs, and sometimes in the course of these affairs they do vexing, annoying, and injurious things. Such acts cannot all be criminal." (*Mahru v. Superior Court, supra,* 191 Cal.App.3d at p. 549; see *Chrisman v. City of Los Angeles* (2007) 155 Cal.App.4th 29, 36-37 [echoing this dicta] (*Chrisman*); *People v. Gentry* (1991) 234 Cal.App.3d 131, 141, fn. 8 [same].) Childs reasons that this language supports his conclusion that section 502 was not intended to apply to employees at all, as a matter of law.

We accept the underlying logic of *Mahru* and the cases that cite it that the Legislature did not intend that all employee misuse of a computer is criminal. However, we do not apply this logic as broadly as Childs does. This dicta raises doubts about criminalizing *routine* computer misuse, but his case involves employee computer misconduct that is anything but routine. The cited principle cannot reasonably be read to decriminalize the acts of a system administrator who used his computer expertise to lock out every other potential user and to wipe out system data if anyone other than him attempted to access his employer's computer system.

Childs also cites us to *Chrisman, supra,* 155 Cal.App.4th at pp. 33-39. In that case, a police officer was terminated from employment for using a police department

---

[33] Since the *Mahru* decision, the Legislature amended section 502 to specifically provide that acts taken at an employer's request are not criminal. (See § 502, subd. (c)(1)-(9); compare with prior § 502, subd. (c) [Stats. 1985, ch. 571, § 1, pp. 2076-2077].)

computer to obtain non-duty related information. The termination was based on a violation of a provision prohibiting unpermitted access to a computer system. (§ 502, subd. (c)(7).) The appellate court reversed, finding that the department had given the officer access to its computer. Subdivision (c)(7) applied only to those who hack into the computer system from without, not to an authorized user who misused that authority. (*Chrisman, supra*, 155 Cal.App.4th at pp. 34-35.) As subdivision (c)(5) does not contain an access requirement, the gravamen of *Chrisman* does not apply to Childs's case.

In dicta, the *Chrisman* court added its reflections on the subdivision (h)(1) "scope of employment" defense. Relying on civil tort case law, it stated that "showing that an employee violated an employer's rules does not determine whether the employee acted within the scope of employment." (*Chrisman, supra*, 155 Cal.App.4th at p. 36; citing *Mary M. v. City of Los Angeles* (1991) 54 Cal.3d 202, 209; *Perez v. Van Groningen & Sons, Inc.* (1986) 41 Cal.3d 962, 967-971.) Applying these tort principles, the *Chrisman* court concluded that "an employer's disapproval of an employee's conduct does not cast the conduct outside the scope of employment." Otherwise, it reasoned, every employee misstep, mistake or misconduct would be criminal under section 502. (*Chrisman, supra*, 155 Cal.App.4th at p. 37.) As the case before us is a criminal one in which tort allocation of the risks and cost of employment injuries is not relevant, the cited language loses some of its force. (See *Mary M. v. City of Los Angeles, supra*, 54 Cal.3d at p. 209; *Perez v. Van Groningen & Sons, Inc., supra*, 41 Cal.3d at pp. 967-971.)

Even if we embrace the logic of the *Chrisman* dicta that an employer's disapproval of an employee's conduct is not definitive on the issue of whether the employee's conduct was within or outside the scope of employment, that would not compel us to find that no employee could ever be convicted of violating subdivision (c)(5) as a matter of law.[34] The misuse of a employer's computer to make searches

[34] At his request, the trial court in Childs instructed the jury on this language taken from *Chrisman*. Apparently, the jury found his conduct more egregious than mere misuse of an employee computer.

without any work-related purpose is not remotely comparable to the computer lockout that Childs accomplished as system administrator of the FiberWAN network.

Childs also calls our attention to *People v. Lawton* (1996) 48 Cal.App.4th Supp. 11.) In that case, a criminal defendant convicted of unauthorized access[35] reasoned that permission granted to use a library computer terminal—its hardware—necessarily conveyed permission to access its software—that is, its computer's operating system. The appellate division of the superior court affirmed. (*Id.* at pp. 14-15; see § 502, subd. (c)(7).) We fail to see how *Lawton* has any bearing on the scope of employment issue before us. This lack of relevance is even more acute, given the fact that the decision applies a version of the statute that predates the 1999 definition of the scope of employment defense in subdivision (h)(1). That language and its meaning is the crux of Childs's claim of error. (See pt. II.C., *ante*.)

We also find *People v. Gentry, supra,* 234 Cal.App.3d 131 unpersuasive. Gentry gained access to confidential files of credit reporting companies and had entered false data to make it more likely that credit would be extended to those who would otherwise be refused. The appellate court affirmed his conviction of a computer crime,[36] concluding that this conduct was "exactly the kind of manipulation of computer data files the statute was designed to prohibit." (*People v. Gentry, supra,* 234 Cal.App.3d at

---

[35] Lawton was also charged with the offense Childs faced—disrupting computer services under subdivision (c)(5)—but his jury did not reach a verdict on this charge. (*People v. Lawton, supra,* 48 Cal.App.4th Supp. at p. 12.)

[36] Gentry was convicted of an access crime under the prior version of section 502 that has since been repealed and replaced. (*People v. Gentry, supra,* 234 Cal.App.3d at p. 40; see prior § 502, subd. (b) [Stats. 1985, ch. 571, § 1, pp. 2076-2077]; see also Stats. 1987, ch. 1499, §§ 2-3, pp. 5782-5786.)

pp. 135, 140-141.) Far from undermining Childs's conviction, this sentiment *supports* it.[37]

F. *Conclusion*

After careful consideration of the statutory language and the case law that Childs cites, we conclude that the Legislature intended for some parts of section 502, subdivision (c) to apply only to external hackers and for some parts—including subdivision (c)(5)—to apply to users who were given lawful access to the computers. Thus, we reject Childs's contention that an employee may not lawfully be convicted of violating subdivision (c)(5), in appropriate circumstances.

III. APPEAL OF CONVICTION

A. *Statutory Vagueness*

1. *General Considerations*

Childs was convicted of violating subdivision (c)(5) of section 502—of knowingly and without permission causing the denial or disruption of computer services to an authorized user of a computer, computer system or computer network. In his first of two consolidated appeals, he challenges two aspects of this statute as unconstitutionally vague. If this claim succeeds, it would render the underlying statute invalid and would bar his conviction.

---

[37] Childs also cites us to two out-of-state cases which are clearly distinguishable from his circumstances. Neither case construes the California law at issue in our case. (See *Arizona v. Moran* (1989) 162 Ariz. 524, 784 P.2d 730; *State v. Olson* (1987) 47 Wash.App. 514; 735 P.2d 1362.) The Arizona case turns on the unique wording its statute banning computer damage, which required an act of commission. (*Arizona v. Moran, supra,* 784 P.2d at pp. 732-734.) By contrast, Childs was charged with disrupting or denying computer services—an offense that, by its terms, may be committed by omission. (See § 502, subd. (b)(8) [denial of access to legitimate users as injury], (c)(5) [disruption or denial of computer services as criminal offense].) In the Washington case, the defendant was charged with computer trespass, an offense that requires unauthorized access. (*State v. Olson, supra,* 735 P.2d at pp. 1363-1364 [Washington statute criminalizes entry into computer system].) Childs's offense does not require access as an element.

Federal and state constitutional due process require a reasonable degree of certainty in statutory language defining a crime. To withstand a facial vagueness challenge, a penal statute must be definite enough that a reasonable person can understand what conduct is prohibited. Otherwise, vague laws may trap innocent persons by not providing *fair notice* of the punishable conduct. The statutory language must also provide definite objective guidelines to police, judges, and juries, in order to prevent arbitrary and discriminatory enforcement of the law. (*People v. Heitzman, supra,* 9 Cal.4th at pp. 199-200; *People v. Guiamelon* (2012) 205 Cal.App.4th 383, 411-412; *People v. Sullivan* (2007) 151 Cal.App.4th 524, 543 [subjective standard]; *People v. Hawkins* (2002) 98 Cal.App.4th 1428, 1439; see U.S. Const., Amend. 14; Cal. Const., art. I, § 15; *Grayned v. City of Rockford* (1972) 408 U.S. 104, 114; see also 17 Cal.Jur.3d (2010) Criminal Law: Core Aspects, § 15, pp. 37-42; 58 Cal.Jur.3d (2012) Statutes, § 21, pp. 397-399.) Childs's vagueness contentions focus on whether he had fair notice of the prohibited conduct. (See *Kolender v. Lawson* (1983) 461 U.S. 352, 357-358.)

When making this vagueness analysis, we begin with the strong presumption that the statute is constitutional. Any constitutional infirmity must be clear and unmistakable. A statute will not be found to be void for vagueness if a reasonable, practical construction can be given to the challenged language. (*People v. Guiamelon, supra,* 205 Cal.App.4th at p. 412; *In re Noreen G., supra,* 181 Cal.App.4th at p. 1374; *People v. Sullivan, supra,* 151 Cal.App.4th at p. 543.) When viewing the statutory language as a whole, if the ordinary meaning of the statutory phrase communicates its meaning, then the statute is not constitutionally vague. (*People v. Estrada* (1995) 11 Cal.4th 568, 581.)

What renders a statute vague is not difficulty in determining whether the crucial term has been proven, but the difficulty of determining what that term means. (*United States v. Williams* (2008) 553 U.S. 285, 286, 306.) A statute does not give fair notice if one of its terms is so vague that a reasonable person of ordinary intelligence must guess at its meaning. However, due process does not require that statutory language be set out with mathematical precision. Even a term that is somewhat imprecise will pass constitutional muster if common understanding and experience renders the language

sufficient to warn against the proscribed conduct. The test is whether the meaning of the language is reasonably ascertainable. (*People v. Sullivan, supra,* 151 Cal.App.4th at p. 543.)

Ordinary terms may find adequate expression in common usage and understanding. (*People v. Sullivan, supra,* 151 Cal.App.4th at pp. 543-544.) We test the statutory language in the context of the charged conduct. (*Grayned v. City of Rockford, supra,* 408 U.S. at p. 112; *People v. Martin* (1989) 211 Cal.App.3d 699, 705.) We also recognize that statutes describing offending conduct arising in a narrowly-defined business setting is subject to a less-strict standard than statutes describing conduct that may be undertaken by a broader population. (See *Papachristou v. City of Jacksonville* (1972) 405 U.S. 156, 162.)

2. *Without Permission*

Childs contends that subdivision (c)(5)'s requirement that prohibited conduct be undertaken "without permission" is unconstitutionally vague. He questions whether his refusal to allow administrative access to the FiberWAN network was done "without permission" because to give the access codes would have violated security policies and instructions from Tong to prevent unqualified persons from having administrative access.

Our inquiry focuses on the language of the statute itself, which we consider in the context of Childs's conduct. (See *Grayned v. City of Rockford, supra,* 408 U.S. at p. 112; *People v. Martin, supra,* 211 Cal.App.3d at p. 705.) Childs's contention rests on his claim that as system administrator, he was responsible for the security of the FiberWAN network. However, by the time Robinson asked for the access codes on July 9, Childs knew that he would *no longer* serve as the network administrator. Someone else would be needed to perform that function. Childs knew that if he did not provide administrative access to DTIS officials, no one would have such access, because he had set up the network with that in mind.

Considered in this context, we are satisfied that no reasonable person with sole administrative access to a city-wide computer network would have thought—once he was removed from his position as system administrator of that network—that the denial of

computer services resulting from his refusal to divulge the information necessary to allow someone else to take over those administrative functions was undertaken *with permission* of DTIS officials. Childs did not act "without permission" in an abstract manner such as by violating a website's unilaterally established terms of use. (See, e.g., *Facebook, Inc. v. Power Ventures, Inc.* (N.D. Cal. July 20, 2010, No. C08-05780) 2010 WL 3291750, pp. 7-12 [unpermitted computer access case].) He refused the direct instruction of his supervisor to divulge information that his employer owned and had the right to know. No reasonable person would have believed that Childs had the city's permission to refuse to provide DTIS officials with administrative access to the system it was responsible for running.

Past cases interpreting the term "without permission" are of little use to us. Most of them actually focus on the question of whether access was with or without permission. (See *Facebook, Inc. v. Power Ventures, Inc., supra,* 2010 WL 3291750, pp. 5-12; *People v. Lawton, supra,* 48 Cal.App.4th Supp. 11, 14-15.) Childs was not charged with an offense requiring proof of unpermitted *access*; instead, he was charged with *disrupting or denying access* of other lawful users of the network without permission to do so. (§ 502, subd. (c)(5).)

To the extent that the reasoning of these cases is applicable to the case at bar, the "without permission" cases support our conclusion. *Overcoming* technical or code-based barriers to gain access to a computer network clearly constitutes access without permission. (*Facebook, Inc. v. Power Ventures, Inc., supra,* 2010 WL 3291750, p. 11; see *People v. Lawton, supra,* 48 Cal.App.4th Supp. at pp. 12-15 [gaining access to software unavailable to general public].) By the same logic, *creating* technical or code-based barriers that prevent the lawful owner of a computer system from gaining access to its network clearly constitute an act undertaken without permission, as that term is used in subdivision (c)(5) of section 502.

In effect, Childs argues that he had the city's permission to lock its officials out of administrative access to its computer network. We reject this interpretation of the "without permission" statutory language as absurd. (See *Gattuso v. Harte-Hanks*

Shoppers, Inc., supra, 42 Cal.4th at p. 567.) Whatever the exact scope and meaning of the term "without permission" might be, it clearly encompasses a refusal to give an employer access to a computer network it owned when the employee's removal from his role as system administrator required him to provide access. (See, e.g., *Skilling v. United States* (June 24, 2010) ___ U.S ___, ___ [130 S.Ct. 2896, 2933].) Construing the challenged term in a reasonable, practical manner, we are satisfied that Childs's conduct fell squarely within the reach of the statute under which he was convicted. (See, e.g., *Findley v. Justice Court* (1976) 62 Cal.App.3d 566, 573; see also *People v. Guiamelon, supra,* 205 Cal.App.4th at p. 412; *People v. Sullivan, supra,* 151 Cal.App.4th at p. 543.) As Childs had fair notice[38] that his conduct was "without permission" of city officials, his vagueness challenge to this aspect of section 502, subdivision (c)(5) fails.

[38] In support of his vagueness claim of error, Childs cites many cases that are of minimal use to us beyond their most general concepts. Most involve statutes implicating First Amendment rights of free speech, press or association, creating the potential for a chilling effect on the exercise of those rights. These cases bear most strongly on the second prong of the vagueness test by raising the specter of overbroad application. (See, e.g., *City of Chicago v. Morales* (1999) 527 U.S. 41, 60 [criticizing broad sweep of anti-gang ordinance]; *Hynes v. Mayor & Council of Oradell* (1976) 425 U.S. 610, 611, 622 [solicitation ordinance cannot turn on police determination of who may conduct political canvassing]; *People v. Mirmirani* (1981) 30 Cal.3d 375, 382-384 [implicating "social and political goals"]; *Katzev v. County of Los Angeles* (1959) 52 Cal.2d 360, 362, 365-368 [ordinance banning "crime comic book" is overbroad]; see *Lanzetta v. New Jersey* (1939) 306 U.S. 451, 452-458 [anti-loitering statute].) By contrast, Childs's claim of error focuses us on the first prong of the vagueness test—whether the statutory language gave him fair notice that he acted "without permission" when he refused to provide the city with administrative access to its computer network. (See *People v. Heitzman, supra,* 9 Cal.4th at pp. 199-200; *People v. Hawkins, supra,* 98 Cal.App.4th at p. 1439.)

3. *Disrupts or Denies*

Childs also challenges the term "disrupts or denies" in subdivision (c)(5) as unconstitutionally vague. He contends that this term is insufficiently certain to give him fair notice that his conduct was criminal. He also reasons that on July 9, the city was merely inconvenienced when he refused to provide administrative access to the FiberWAN network. Before trial, Childs made a similar argument—that because the city suffered no lapse or interference with basic computer functions, the prosecution could not prove that he caused any denial or disruption of computer services. Rejecting this contention, the trial court denied his motion to dismiss the subdivision (c)(5) charge. (§ 995.)

We also reject his vagueness contention. The dictionary definition of a challenged term can be useful in this inquiry. (See, e.g., *People v. Hawkins, supra,* 98 Cal.App.4th at p. 1439.) The word "deny" comes from a Latin root, meaning "to negate," or causing to be ineffective. (See Webster's 11th Collegiate Dict. (2004) pp. 334, 829.) To "disrupt" is to "throw into disorder" or "to interrupt the normal course." (*Id.*, at p. 362.)

In its most literal sense, Childs's refusal to provide the city with administrative access to the FiberWAN network constituted multiple denials or disruptions of the city's computer system. DTIS had no ability to assign a new system administrator for the network. It could not remove Childs from ongoing access to the network. DTIS could not make administrative changes to the network, add new city departments to it or

---

This distinguishing factor also applies to the two California cases that specifically discuss the meaning of the term "permission." In rejecting gang-related conditions of probation barring a probationer's presence at certain locations without a probation officer's permission, courts express the concern that they give the officer too much discretion to enforce court-ordered conditions of probation. These cases focus on the potential for arbitrary enforcement of the conditions of probation and their potential to impinge on lawful rights of association are less useful to us than Childs suggests. (*In re E.O.* (2010) 188 Cal.App.4th 1149, 1152, 1155 & fn. 3; *People v. Leon* (2010) 181 Cal.App.4th 943, 954.) A third case from the United States Supreme Court turned on the internal inconsistency of statutes meant to be read together and is likewise distinguishable from the challenge Childs makes. (See *United States v. Cardiff* (1952) 344 U.S. 174, 176-177.)

monitor its integrity from July 9 to July 21. In each of these ways, Childs denied computer services to DTIS within the meaning of subdivision (c)(5) of section 502.

Subdivision (c)(5)'s mens rea requirement that Childs acted knowingly also blunts any fair notice issue pertaining to the term "disrupt or denial." (See, e.g., *Skilling v. United States, supra,* ___ U.S at p. ___ [130 S.Ct. at p. 2933]; see *People v. Hawkins, supra,* 98 Cal.App.4th at pp. 1437-1439 [awareness or intention required].) He concedes that the statutory intent requirement that he act "knowingly" modifies the term "disrupts or denies." The jury was instructed that it had to find that his disruption or denial of computer services was knowingly done. By finding that Childs knowingly disrupted or denied computer services, it rejected the conclusion that he committed a crime by accident or misfortune. (See *People v. Coria* (1999) 21 Cal.4th 868, 876; *People v. Hawkins, supra,* 98 Cal.App.4th at p. 1439.) His criminal responsibility was triggered by his knowledge that by refusing to allow anyone else to have administrative access to the network—by retaining "the keys to the kingdom" even after being removed as administrator of FiberWAN, suspended from city employment and arrested—he denied DTIS its full use of that computer network.

Childs makes a related factual argument that is also groundless. In support of his claim that the city was merely inconvenienced by his actions, he asserts that the evidence established that he continued to be available to administer the FiberWAN network after July 9. He was not terminated from city employment on that date, but expected that his employment would continue at least until the scheduled July 18 administrative review hearing. Childs argues that a reasonable person could not be expected to know on July 9 that Robinson would not ask him to resume his network administrator responsibilities after that date or that the July 18 review hearing would not occur because he would be under arrest by that time.

This argument ignores other facts that the jury appears to have found more persuasive than that which Childs cites to us. Before July 9, Childs set up the FiberWAN system so that no one else had administrative access to it, deliberately locking DTIS out of its computer network. Any attempt to gain administrative access to the network—by

other DTIS employees, by Childs's supervisors, or by outside vendors retained to support it—would have erased its contents. Even after being removed as network administrator and after being arrested on July 12, Childs refused to allow others to have administrative access to the network. At that point, no reasonable person would have believed that DTIS would ask him to resume his administrator role. By July 15, he had been suspended without pay, making it even clearer that he would not be allowed access to the network. Viewed in context, we are satisfied that Childs had fair notice that his actions constituted a denial or disruption of the city's computer services.[39] We reject this due process challenge to his conviction.

B. *Privilege Against Self-Incrimination*

Next, Childs contends that the trial court violated his privilege against self-incrimination by admitting evidence that he failed to divulge his user name and password after being arrested. He sets the date of his arrest at July 9 after Inspector Ramsey informed him that his refusal to provide FiberWAN administrative access to the city could subject him to criminal prosecution. At this point, Childs reasons that he had a constitutional right to remain silent—to decline to provide the information that the city sought. He urges us that to conclude that using his July 9 through July 21 silence against him deprived him of a fair trial. (See U.S. Const., 5th Amend.)[40]

As a preliminary matter, we reject Childs's claim that he was under arrest once Inspector Ramsey joined the July 9 meeting. At that meeting, Ramsey asked Childs to

---

[39] In his reply brief, Childs also suggests that the term "computer services" is vague. He did not raise this claim of error in his opening brief. An appellant may not raise a new issue in a reply brief as to do so deprives the respondent of a fair opportunity to respond to it. (*People v. Zamudio* (2008) 43 Cal.4th 327, 353-354; see *Varjabedian v. City of Madera* (1977) 20 Cal.3d 285, 295, fn. 11; see also 9 Witkin, Cal. Procedure, *supra,* Appeal, § 723, pp. 790-791.)

[40] In his unsuccessful motion for new trial, he argued that he was prosecuted for failing to provide the sought-after information after he was arrested, in violation of his privilege against self-incrimination. (See *Doyle v. Ohio* (1976) 426 U.S. 610, 617-618.) The prosecution's opposition to the motion for new trial noted that it had complied with a trial court order that it make no closing argument comment about Childs's post-arrest silence.

cooperate with DTIS, saying that if he did not do so, his refusal would constitute a denial of computer services for which he could be criminally liable. As Childs admitted at trial, Ramsey told him that he was *not* under arrest at that time. This encounter was a detention, not an arrest—a fact which Childs also acknowledged when he signed a release of the city property he relinquished. He first invoked his privilege against self-incrimination at the time of his July 12 arrest.

Regardless of when Childs was arrested, his claimed privilege against self-incrimination defense does not apply. This privilege bars the state from compelling a person to be a witness against him or herself. (*Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cty.* (2004) 542 U.S. 177, 189; *People v. Kurtenbach* (2012) 204 Cal.App.4th 1264, 1283.) It does not bar all compelled disclosures, even if those disclosures might lead to criminal prosecution. (See, e.g., *California v. Byers* (1971) 402 U.S. 424, 431-432 [one involved in accident may be required to stop and give identifying information]; *United States v. Wade* (1967) 388 U.S. 218, 221 [accused may be compelled to speak during physical lineup]; *United States v. Sullivan* (1927) 274 U.S. 259, 262-264 [one may be lawfully required to identify sources of income on tax returns, even when that income was illegal]; *People v. Kurtenbach, supra,* 204 Cal.App.4th at pp. 1282-1287 [one may be required to disclose an event affecting insurance benefits].)

To qualify for Fifth Amendment protection, a communication must be testimonial. In some circumstances, a criminal defendant may invoke the privilege against self-incrimination as a defense if the prosecution is based on the defendant's failure to comply with a statute requiring disclosure of incriminating information. (*People v. Kurtenbach, supra,* 204 Cal.App.4th at pp. 1283-1284; see *California v. Byers, supra,* 402 U.S. at p. 432.) However, the United States Supreme Court has set limits on the circumstances under which a criminal defendant may use this defense. Courts resolve the tension between a state's demands for disclosures and the defendant's privilege against self-incrimination by balancing the public need against the individual's constitutional protection. Applying this balancing test, the United States Supreme Court has determined that the privilege does not apply if the incriminating disclosure is required for

compelling, broadly applied reasons unrelated to criminal law enforcement. The defense does not apply when a statute requires disclosure in what is essentially a noncriminal context. This analysis does not focus on whether the disclosure requires an incriminating statement, but whether, generally speaking, the statutory requirement will result in disclosure of incriminating information. (*People v. Kurtenbach, supra*, 204 Cal.App.4th at p. 1284.)

Courts use a three-part inquiry when conducting this balancing test. First, we consider whether the statute targets a highly-selective group inherently suspected of criminal activity. (*People v. Kurtenbach, supra,* 204 Cal.App.4th at p. 1285.) The disclosure required of Childs to allow DTIS administrative access to its computer system was not inherently criminal. Second, we determine whether the statute regulates an activity permeated with criminal statutes. (*Id.* at pp. 1285-1286.) Section 502, subdivision (c)(5) regulates the use of computer systems—a legal activity, not an illegal one such as gambling or the sale of narcotics. (See *People v. Kurtenbach, supra*, 204 Cal.App.4th at p. 1286.) Third, we weigh whether the statute requires disclosures for compelling, broad-based reasons unrelated to criminal law enforcement. (*Id.* at p. 1286.) The broad purpose of section 502 is to avoid disruption or denial of vital computer services. (§ 502, subd. (a); *People v. Hawkins, supra,* 98 Cal.App.4th at p. 1440.) The disclosures required by this statute serve compelling business and governmental interests, not law enforcement. (See *People v. Kurtenbach, supra,* 204 Cal.App.4th at p. 1286.)

All three of the *Kurtenbach* factors weigh against the application of the privilege against self-incrimination in the case before us. Thus, we conclude that for DTIS to require its outgoing computer system administrator to reveal access codes necessary to allow the new system administrator to perform those functions is not the type of disclosure protected by the privilege against self-incrimination.

C. *Instructions*

1. *Definition of Terms*

a. *Instruction Given*

Childs also raises several instructional challenges. He first argues that the trial

court's instruction defining the charged offense was inadequate because it failed to define the terms "authorized user," "without permission," "disrupts or denies," "computer services," "within the scope of his employment," and "reasonably necessary to the [employee's] work assignment."[41]

The trial court in a criminal case has a sua sponte duty to instruct the jury on general principles of law relevant to the issues raised by the evidence—those principles necessary to the jury's understanding of the case. (*People v. Roberge* (2003) 29 Cal.4th 979, 988; *People v. Estrada, supra,* 11 Cal.4th at p. 574.) Childs was charged with knowingly and without permission disrupting or denying computer services to an authorized user of a computer, computer system, or computer network. (See § 502, subd. (c)(5).) The trial court instructed the jury on those elements in an instruction it crafted.[42] That instruction paralleled the language of subdivision (c)(5); defined the terms "computer network," "computer services," and "computer system" as set out in

[41] In support of this argument, Childs improperly cites an appellate case in which the California Supreme Court granted review. (See *People v. Schade* (1994) 30 Cal.App.4th 1515, review granted Sep. 15, 1994, S040968); see also Cal. Rules of Court, rules 8.1105(e)(1), 8.1115(a).)

[42] Although the record indicates that the instruction was a modified form of CALCRIM No. 1946, there is no standard instruction with that number. (See CALCRIM (2013) p. 45.) The parties agree that the trial court wrote the instruction for this case.

subdivision (b)(2), (4) and (5); and instructed the jury on the scope of employment defense as specified in subdivision (h)(1).[43]

If the Legislature defines a term, courts are usually bound by that definition. (*People v. Zeigler, supra,* 211 Cal.App.4th at p. 650.) In most cases, instructing the jury on the statutory definition of an offense is sufficient if the jury would have no difficulty understanding that language. The meaning of a statute is adequately conveyed by its express terms if the words used are commonly understood by those familiar with the English language and the terms are not used in a technical sense peculiar to the law. A term with a legal, technical meaning must be clarified sua sponte if it has a definition that differs from the nonlegal meaning that might be ascribed to the same terms in common parlance. (*People v. Rodriguez, supra,* 28 Cal.4th at pp. 546-547; *People v. Estrada, supra,* 11 Cal.4th at pp. 574-575.) If the trial court instructs the jury on the statutory language and the defendant does not seek amplification of the terms used in the statute,

[43] The trial court gave this instruction to the jury: "The defendant is charged . . . with disrupting or denying of computer services to an authorized user. To prove the defendant is guilty of this crime, the People must prove: [¶] 1. the Defendant knew that he disrupted or denied computer services; [¶] 2. the Defendant knew that the disruption or denial was to an authorized user to the computer, computer system, or network; [¶] AND 3. the Defendant did not have permission. [¶] 'Computer Network' means any system that provides communication between one of more computer systems and input/output devices, including but not limited to, display terminals and printers connected by telecommunication facilities. [¶] 'Computer services' includes but is not limited to, computer time, data processing, storage functions, or other uses of a computer, computer system, or computer network. [¶] 'Computer system' means a device or collection of devices, including supporting devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, [or] input data. [¶] The knowing disruption or denial of computer services to an authorized user of a computer, computer system or computer network without permission is not criminal if committed by a person within the scope of his or her lawful employment. If you find the aforementioned elements to have been proved beyond a reasonable doubt, the People have the further burden of proving beyond a reasonable doubt that the defendant was not acting within the scope of his employment when committing the knowing disruption or denial of computer services to an authorized user without permission. If the People have not met this burden, you must find the defendant not guilty of this crime."

the instruction is sufficient. The trial court has no sua sponte duty to clarify terms that are not used in a legal, technical manner. (*People v. Rodriguez, supra,* 28 Cal.4th at p. 546; *People v. Estrada, supra,* 11 Cal.4th at pp. 574, 581.)

The People argue that Childs forfeited the right to challenge all of these terms as ambiguous because he failed to seek clarification of them in the trial court.[44] The record supports the conclusion that his written proposed jury instruction did not seek to amplify the terms "authorized user," "without permission," "disrupts or denies" as he argues on appeal.[45] Thus, he has waived the right to challenge these claims of instructional error that he failed to bring to the trial court's attention. (*People v. Hart* (1999) 20 Cal.4th 546, 622; *People v. Bolin* (1998) 18 Cal.4th 297, 326; *People v. Stone* (2008) 160 Cal.App.4th 323, 331.)[46] We address those issues that were properly preserved for our consideration on appeal.

---

[44] The People also argue that Childs agreed to the instruction given, suggesting that the invited error doctrine applies. In light of our finding of forfeiture, we need not determine that additional question.

[45] Much of the discussion of the jury instructions appears to have taken place off the record. Thus, Childs cannot demonstrate that he made any verbal request for clarification of any of the statutory terms. As the appellant, he has the burden of proving that he is entitled to relief on appeal. (See *People v. Davis* (1996) 50 Cal.App.4th 168, 172-173 [appellant must affirmatively demonstrate error and cannot rely on silent record].)

[46] Even without a trial court objection, we *may* review any instruction given that affects the substantial rights of the defendant. (§ 1259; *People v. Gray* (2005) 37 Cal.4th 168, 235.) We are not *required* to do so, and nothing in Childs's arguments about these terms persuades us that his substantial rights were affected by the use of these statutory terms without further definition.

b. "*Computer Services*"[47]

Childs argues that a major issue in this case was the meaning of the term "disrupts or denies computer services." Childs took the position there was no disruption or denial of services because the system continued to be available to end users and administrative services were disrupted only after he was arrested. The jury instruction defined computer services only in terms of the statutory definition. This was inadequate, Childs contends, because the jury asked for a "better deffinition [sic] of the term computer services." Childs further argues the trial court erred by failing to provide a more detailed explanation, rather than referring them to the definition already given. When the request is viewed in context, however, it is clear that no error occurred.

On the first full day of jury deliberations, a hint of trouble emerged. The jurors sent a note to the trial court, asking what to do if one juror refused to discuss the case. The court reinstructed the jurors about their duty to talk with each other about the case. (See CALCRIM No. 3550.) At the close of that day's deliberations, the jurors were ordered to deliberate through their lunch the next day. Juror No. 12 protested, but the judge cut off his comments, fearing that he might reveal the jury's thought processes arising during deliberations in violation of specific instructions not to do so. (CALCRIM No. 3550.)

On following day, Juror No. 12 filed a written objection to the court's order that he have lunch while continuing to deliberate. Insisting on a lunch break, he suggested that if he did not get his way, he would become angry and that this would "probably" affect his ability "to render an impartial verdict." He also noted that the jury instructions were "causing jury confusion." In a troubling aside, the letter stated that the remaining

[47] Childs requested the following as part of his Section 502 instruction: "Before a defendant can be found to have knowingly disrupted or denied computer services to an authorized user of a computer, computer system, or computer network he must have interacted physically or electronically with the computer, computer system, or computer network and that such interaction must have caused the disruption or denial of computer services." Childs's argument regarding this instruction focuses only on the definition of computer services, and not on any other aspect of this rejected instruction.

jurors had concluded that Childs was guilty and that Juror No. 12 felt pressured to agree with them.

The trial court read the letter into the record, concluding that it violated Juror No. 12's duty not to reveal the deliberations process. It realized that the juror might have to be removed. Juror No. 12 was brought into court and advised that his discussion of the jury's deliberations was improper.

On his request for a lunch break, Juror No. 12 sought to continue his practice of taking a lunchtime nap in his car. He needed this for his comfort, not because of any physical issues. When the judge offered to take a short lunch break, Juror No. 12 found that insufficient; because he was disabled, he needed time to get to and from the place where he got his lunch. As he had in his letter, Juror No. 12 stated in court that if he did not get his lunch break, he would not have an open mind, but would be upset and angry while deliberating. The trial court allowed the jurors to have 30 minutes for lunch and stated that lunch would be provided to him. Juror No. 12 protested that he did not want lunch provided to him; he wanted an hour-long lunch break.

After ordering Juror No. 12 from the courtroom, the trial court noted that the juror had an unspecified physical difference. He admitted that his desires were based on comfort and were unrelated to a physical disability. She also stated that Juror No. 12 had indicated that if she did not allow him his lunch break, he would refuse to deliberate. The trial court expressed concern that he sought to control the pace of deliberations for personal reasons, not because of any needed accommodation related to disability. She was also concerned because Juror No. 12 had revealed the content of deliberations. The prosecution asked that Juror No. 12 be removed from the jury. The trial court ordered the jurors to continue deliberating, and waited to see if Juror No. 12 would refuse to participate.

While the trial court considered the request to remove Juror No. 12, the jury asked for a "better" definition of "computer services." Without objection, the trial court instructed the jurors to review the definition it had already given. Soon, the jurors sent another note to the judge, this one stating: "We are unable to even get past the definitions

on the jury instructions. One juror is refusing to abide by the court[']s definitions and instructions and inserting their own instead."

The trial court removed Juror No. 12 for failing to follow its instructions and for threatening to render a non-impartial verdict. An alternate juror replaced Juror No. 12 and the jury was instructed to begin deliberations anew. The trial court declined to address the pending juror question for a definition of computer services; as the deliberations would begin all over again, that inquiry was deemed irrelevant. The trial court asked the new jurors if they had done any investigation of the meaning of the term "computer services," but no one indicated that they had. That afternoon, the new jury reached its verdict.

The law that applies when jurors request clarification of instructions during deliberations is well-settled. If deliberating jurors require more information on any pertinent point of law, the jurors must be brought into court and the required information must be given to the jurors in the presence of both sides. (§ 1138.) The trial court has a mandatory duty to clear up any confusion created by its original instructions. (*People v. Gonzalez* (1990) 51 Cal.3d 1179, 1212, superseded by statute on another point in *Barnett v. Superior Court* (2010) 50 Cal.4th 890, 898.) When the instructions already given—particularly those based on statutory language—are full and complete, a trial court faced with a request for clarification is not always required to elaborate on those instructions. The court has discretion to determine what additional explanation is needed. (*People v. Beardslee* (1991) 53 Cal.3d 68, 97; *People v. Gonzalez, supra,* 51 Cal.3d at p. 1213.)

In this case, it is reasonably apparent that the jury's request for clarification about the meaning of the term "computer services" was generated more out of frustration with Juror No. 12's refusal to abide by the earlier instructions than actual confusion about the meaning of the term. In either event, when that juror was removed we presume that the reconstituted jury began deliberations anew, as instructed. (*People v. Fuiava* (2012) 53 Cal.4th 622, 716.) No request for clarification came from the new jury. In these circumstances, we conclude that the trial court properly exercised its discretion not to

offer further instruction to the new jury on the meaning of "computer services." (See *People v. Gonzalez, supra,* 51 Cal.3d at p. 1213.)[48]

c. *"Scope of Employment" and "Reasonably Necessary to Work Assignment"*

Childs is also critical of the trial court for rejecting his proposed instruction defining terms applicable to a statutory defense to the charged crime. One cannot lawfully be convicted of disrupting or denying computer services while acting "within the scope of his or her lawful employment." For purposes of this defense, a person is deemed to have acted within the scope of his or her employment "when he or she performs acts which are reasonably necessary to the performance of his or her work assignment." (§ 502, subd. (h)(1).)

A trial court has a sua sponte duty to instruct on an applicable defense on which the defendant relies. *(People v. Stewart* (1976) 16 Cal.3d 133, 140.) The trial court instructed the Childs jury on this defense using the statutory language. (See § 502, subd. (h)(1).) At Childs's request, it added that an employer's disapproval of an employee's conduct does not determine whether the employee acted outside the scope of employment. It rejected his other requests to define conduct within the scope of employment.[49]

On appeal, Childs contends that the refusal of his complete proposed instruction on the meaning of the terms "within the scope of his employment" and "reasonably

---

[48] For a related discussion about Juror No. 12, see pt. III.D., *post*.

[49] Childs sought this additional instruction: "Conduct is within the scope of employment if: (a) It is reasonably related to the kinds of tasks that the employee was employed to perform; or [¶] (b) It is reasonably foreseeable in light of the employer's business or the employee's job responsibilities. [¶] (c) An employee's unauthorized conduct may be within the scope of employment if the conduct was committed in the course of a series of acts authorized by the employer or the conduct arose from a risk inherent in or created by the enterprise. [¶] (d) An employee's wrongful or criminal conduct may be within the scope of employment even if it breaks a company rule or does not benefit the employer. Conduct that violates an employee's official duties or disregards the employer's express orders may nonetheless be within the scope of employment."

necessary to his work assignment" left the jurors with an insufficient understanding of the technical, legal meaning of the statutory language. He argues that the trial court erred by rejecting his proposed language, which he asserts was an accurate statement of the law taken from applicable cases. (See *Chrisman, supra,* 155 Cal.App.4th at pp. 36-37; *Mahru v. Superior Court, supra,* 191 Cal.App.3d at p. 549.) He reasons that because the instruction given did not fully or accurately reflect those case holdings, it was insufficient, leaving him vulnerable to an erroneous conviction by effectively depriving him of a statutory defense to the charged conduct.

We disagree. To begin with, the phrase "reasonably necessary to the performance of his work assignment" is *itself* the statutory definition of "within the scope of employment." The instruction given thus accurately relates that defense as set forth in the statute (*People v. Estrada, supra,* 11 Cal.4th at p. 574), which was then embellished with language requested by Childs, to the effect that an employer's approval or disapproval of the acts in question is not determinative of the scope of employment. The remaining portions of the proposed instruction are not a correct statement of law. (*People v. Gurule* (2002) 28 Cal.4th 557, 659.) Childs relies on *Mahru, Chrisman, Lawton,* and *Gentry* as elucidating the "technical, legal" meaning of these statutory terms. Neither *Lawton* nor *Gentry* involved scope of employment issues, and we have already discussed and distinguished *Mahru* and *Chrisman,* which are not controlling here. (See Section II.E, *supra*.)

As an example, Childs asked the court to instruct that "an employee's wrongful *or criminal* conduct may be within the scope of employment even if it breaks a company rule or does not benefit the employer." [Italics added.] This was taken from the discussion in *Chrisman, supra,* 155 Cal.App.4th at page 36, of cases analyzing the term "within the scope of employment" for purposes of imposing vicarious liability on an employer for the wrongful acts of its employee. (See, *Mary M. v. City of Los Angeles* (1991) 54 Cal.3d 202; *Perez v. Van Groningen & Sons, Inc., supra,* 41 Cal.3d at pp. 967-970.) The doctrine of respondeat superior is designed to address three policy concerns: "(1) to prevent recurrence of the tortious conduct; (2) to give greater assurance of

compensation *for the victim*; and (3) to ensure that the *victim's losses* will be equitably borne by those who benefit from the enterprise that gave rise to the injury." (*Mary M. v. City of Los Angeles, supra*, 54 Cal.3d at p. 209 [italics added].) Thus, it makes sense to apply the proposed principle in circumstances where the victim of an employee's wrongful conduct is seeking to hold the employer liable. Applying that principle under the facts of this case—where the employer *is* the employee's victim—would run the danger of nullifying the application of section 502, subdivision (c)(5) entirely.

2. *Unauthorized Access*

Childs also argues that the instructions defining the offense described in section 502 failed to include an essential element of that offense—the unauthorized access to a computer. The failure to instruct on an element of an offense violates a criminal defendant's federal and state constitutional rights. A criminal defendant may challenge such an omission even if no objection was raised to the instruction in the trial court. (*People v. Tillotson* (2007) 157 Cal.App.4th 517, 538.) However, we have found the underlying assumption to be incorrect. (See pt. III.A.3, *ante*.) As such, we necessarily reject his instructional challenge.

3. *Adoptive Admission*

Next, Childs contends that the trial court erred in instructing the jury on adoptive admissions. Evidence of a declarant's statement offered against a party is not inadmissible hearsay if the statement is one that the party—with knowledge of its content—has by words or other conduct manifested an adoption or belief in its truth. (Evid. Code, § 1221; *People v. Fauber* (1992) 2 Cal.4th 792, 851.) At the prosecution's request and over Childs's objection, the trial court instructed that if "you conclude that someone made a statement outside of court that accused the defendant of a crime or tended to connect the defendant with the commission of the crime and the defendant did not deny it, you must decide whether each of the following is true: [¶] One, the statement was made to the defendant or made in his presence. [¶] Two, the defendant heard and understood that statement. [¶] Three, the defendant would under all circumstances naturally have denied the statement if he thought it was not true. [¶] And four, the

defendant could have denied it but did not. [¶] If you decide that all of these requirements have been met, you may conclude that the defendant admitted the statement was true. [¶] If you decide that any of the requirements has not been met, you must not consider either the statement or the defendant's response for any purpose." (CALCRIM No. 357.)

The trial court found sufficient evidence to give this instruction because Ramsey testified that on July 9, Childs did not react when he explained that failure to cooperate with the city could constitute a violation of section 502. Childs admitted that when he was advised that his conduct could be criminal, he did not provide the access that DTIS officials sought. Instead, he lied and gave them false information.[50]

On appeal, Childs argues that the instruction should not have been given because a reasonable jury could not have found that either he understood the contents of Ramsey's statement or that he manifested an adoption or belief in the truth of that statement by his words or conduct. (See *People v. Lewis* (2008) 43 Cal.4th 415, 497; *People v. Maki* (1985) 39 Cal.3d 707, 712.) He reasons that section 502 is so complex that he needed the advice of legal counsel to parse its meaning, such that he could not be said to have understood the import of Ramsey's statement at the time it was made. He also contends that the evidence did not show that he adopted Ramsey's statement by failing to respond to it. Finding himself in the situation he was in on July 9, he argues that a reasonable person might choose not to respond to the statement, fearing that he might blunder into some incriminating response.

To render evidence of an adoptive admission admissible, it is sufficient if the evidence supports a reasonable inference that an accusatory statement was made under circumstances affording Childs a fair opportunity to deny it, without implicating his privilege against self-incrimination. If a statement is made under circumstances that would normally call for a response if it were untrue, then the statement is admissible for

[50] Childs testified that Ramsey told him that failure to provide access to the police department network could be a violation of section 502. He told the jury that after he heard Ramsey say this, he provided access to the police department's network.

the limited purpose of showing Childs's reaction to it. His reaction may constitute a tacit admission of the truth of the statement. Once the evidence is admissible, the factual issue of whether or not his conduct actually constituted an implied or adoptive admission then becomes a matter for the jury to decide. (See *People v. Geier* (2007) 41 Cal.4th 555, 590-591; *People v. Riel* (2000) 22 Cal.4th 1153, 1189-1190; *People v. Fauber, supra,* 2 Cal.4th at pp. 851-853; *People v. Edelbacher* (1989) 47 Cal.3d 983, 1011, disapproved on another ground in *People v. Loyd* (2002) 27 Cal.4th 997, 1007, fn. 12, 1010.)

To a great extent, Childs's claim of error is based on his assertion that his silence was construed against him in violation of the privilege against self-incrimination or is grounded in his claim that subdivision (c)(5) was too ambiguous to be understood. As we have already rejected these contentions, these underpinnings of this instructional challenge is also unavailing. (See pts. III.A. & III.B., *ante*.)

The remainder of his instructional challenge also fails. The adoptive admission instruction is properly given if specific foundational facts can be inferred from the record. The record contains evidence from which a reasonable juror could infer that Childs understood that his continued refusal to provide administrative access to the FiberWAN network to city officials could constitute a crime. The jury could reasonably infer from this evidence that Childs's failure to provide the sought-after access codes constituted an admission that he had committed a crime.

Even if the jurors found the facts to be as the prosecution urged them to find, the instruction did not *require* the jurors to find that Childs admitted by his silence that he had committed a crime. It merely *permitted* the jury to make this further inference. (See *People v. Medina* (1990) 51 Cal.3d 870, 891; see also *People v. Zavala* (2008) 168 Cal.App.4th 772, 780.) If a different inference was also raised by the record, Childs was entitled to argue that this inference was more credible. Even if Childs could offer a reasonable explanation for his silence, that fact weighs into the jury's determination. It does *not* render the evidence inadmissible. (See, e.g., *People v. Geier, supra,* 41 Cal.4th at pp. 590-591.)

As the circumstances warranted presenting the evidence to the jury to let it decide what weight to give to that evidence, the trial court correctly instructed the jury on how to consider this adoptive admission evidence. *(People v. Riel, supra,* 22 Cal.4th at p. 1190.) The jury was instructed to determine whether Childs made an admission, to evaluate how much weight to give to it, and to view any evidence of that out-of-court statement with caution. (CALCRIM No. 358.) It was also instructed that Childs could not be convicted on the basis of the adoptive admission alone, but that it could rely on this evidence only if the jury concluded that other evidence showed that the charged crime was committed. (CALCRIM No. 359.) (See *People v. Fauber, supra,* 2 Cal.4th at p. 853.) We presume that jurors understand, correlate, and follow the trial court's instructions. (*People v. Sanchez* (2001) 26 Cal.4th 834, 852.) The trial court did not err by giving this instruction.

Even if we assume arguendo that giving this instruction was error, any error was clearly harmless. Childs is entitled to reversal of his criminal conviction only if our examination of the entire case makes it reasonably probable that he would have obtained a more favorable outcome in the absence of the error. (*See People v. Watson* (1956) 46 Cal.2d 818, 836-837; see also *People v. Flood* (1998) 18 Cal.4th 470, 502-503; *People v. Elize* (1999) 71 Cal.App.4th 605, 616.) To establish a reasonable probability, he must show a reasonable chance of a different outcome, not merely an abstract possibility. (*People v. Superior Court (Ghilotti)* (2002) 27 Cal.4th 888, 918; see *College Hospital Inc. v. Superior Court* (1994) 8 Cal.4th 704, 715.) The reasonable probability must be such that it undermines our confidence in the jury's verdict. (See *Strickland v. Washington* (1984) 466 U.S. 668, 693-694; *People v. Jenkins* (2000) 22 Cal.4th 900, 954; *In re Sassounian* (1995) 9 Cal.4th 535, 544.)

The challenged evidence—an implied admission to an out-of-court statement which the jury was merely permitted to infer—paled in significance to the direct admissions that Childs himself gave while testifying in court, under oath, before the jury.

Given his admissions on the witness stand, the weight to be given to an adoptive admission that the jury might have inferred from his failure to respond to Ramsey's statement is clearly less significant. Even if this were not so, much of Childs's prejudicial error argument turns on assertions that we reject—that the jury was confused about the meaning of "computer services" and that section 502, subdivision (c)(5) was ambiguous. (See pts. III.A. & III.C.1.b., *ante*; see pt. III.D., *post*.)

Contrary to Childs's assertion, this was not a close case. The evidence that he locked DTIS out of administrative access to its FiberWAN network was overwhelming. At trial, he admitted as much. He admitted that when city officials attempted to regain access to the computer system, he lied by denying that he had backup configurations. He lied again by providing incorrect passwords. He admitted that he had disabled the password recovery feature on the CE devices. He admitted that he had configured core network devices to run only on VRAM without consulting DTIS management. He admitted that he had disabled the console ports on these core devices. He admitted that as configured, these core devices would shut down and their contents would be erased if anyone attempted to access them or if the system was powered down, even by accident. If required to make a prejudicial error analysis, we would find any error to be harmless.

D. *Dismissal of Juror No. 12*

1. *Facts*

Next, Childs argues that the trial court erred in dismissing Juror No. 12 during deliberations over Childs's objection.[51] He contends that the trial court did not remove the juror because he was unable to perform his duties, but because he had doubts about the sufficiency of evidence. Childs reasons that this removal violated his rights to a jury trial and to due process, compelling reversal. (U.S. Const., 6th, 8th & 14th Amends.; Cal. Const., art. I, §§ 15-16; § 1089.)

We have already set out some of the facts related to this issue. (See pt. III.C.1.b.i., *ante*.) During the initial round of deliberations, one juror reportedly refused to discuss his opinion of the case with the other jurors. (See CALCRIM No. 3550.) It soon became clear that Juror No. 12—who was physically disabled—was the juror in question. In a letter, he protested the trial court's order to deliberate during the jury's lunch period.

His letter suggested two areas of concern for the trial court. First, Juror No. 12 reported that the other eleven jurors had voted to convict and he was the lone holdout for acquittal. This report of the jury's thought processes during deliberations violated the trial court's instructions not to reveal how he or any other juror voted on guilt or innocence unless the court asked for this information. Juror No. 12 also hinted that he would be angry, biased, and unable to render an impartial verdict if the trial court did not allow him the lunch break he wanted.

The trial court found that Juror No. 12's letter violated his duty not to reveal the deliberations process, observing that he might have to be removed. The judge conducted an investigation, questioning Juror No. 12. In his oral explanation, he repeated that if he

[51] In support of this argument, Childs's counsel referred to an appellate case in which review was granted. (See *People v. Valot* (2002) 103 Cal.App.4th 1247, review granted Feb. 25, 2003, remanded May 14, 2003, S112450.) This is improper. (See Cal. Rules of Court, rules 8.1105(e)(1), 8.1115(a).)

was not comfortable with the lunch arrangements, "I don't think [I] am going to [have an] open mind. I am going to be upset. I will be angry, and I don't believe that [anyone] needs this kind of person in deliberating."

Rejecting Childs's argument that the juror merely sought an accommodation, the trial court found that Juror No. 12 wanted a longer lunch break for personal reasons that were unrelated to his disability. It expressed concern that he sought to control the pace of deliberations for personal reasons, not because of any need for accommodation related to disability. The court was concerned that Juror No. 12 was refusing to deliberate if not given the lunch break he sought. Finally, it was critical of Juror No. 12 for revealing the content of jury deliberations. After the prosecution asked that the juror be removed, the trial court ordered the jurors to continue deliberating and waited to "see what happens." Soon, the jurors made two inquiries which, when read together, suggested that Juror No. 12 was refusing to deliberate. Outside the presence of the jury, Childs argued that Juror No. 12—who he knew was the only juror who would have not found him guilty—was open-minded and wanted to continue deliberating. To this, the trial court added a caveat: "If I don't anger him."

Juror No. 12 was removed from the jury. In a lengthy explanation, the trial court stated that it could not allow a juror who had already violated its instructions to become angry and retaliate by failing to be fair and impartial. She based his removal on the violation of his duty not to comment on the thought processes of the deliberations and on his threat to render a biased verdict if he disagreed with the trial court's orders. (See § 1089.)

2. *Legal Principles*

For good cause, if a trial court finds a seated juror is unable to perform his or her duty, it may order that juror to be discharged and replace him or her with an alternate juror.[52] (§ 1089; *People v. Fuiava*, *supra*, 53 Cal.4th at p. 710.) If improper, this discharge may implicate a criminal defendant's federal and state constitutional rights to a jury trial, to due process, and to an unanimous verdict. (U.S. Const., 6th, 8th & 14th Amends.; Cal. Const., art. I, §§ 15-16; see *People v. Karapetyan* (2003) 106 Cal.App.4th 609, 621; *People v. Fuiava, supra,* 53 Cal.4th at p. 710; *People v. Barnwell* (2007) 41 Cal.4th 1038, 1052.) The discharge of a juror cannot be based on his or her doubts about the sufficiency of the prosecution's evidence, as that would violate the defendant's right to a unanimous jury. (*People v. Engelman* (2002) 28 Cal.4th 436, 446; *People v. Cleveland* (2001) 25 Cal.4th 466, 481-483; *People v. Karapetyan, supra,* 106 Cal.App.4th at p. 621.) If the substitution of a juror during deliberations is made for good cause, then the removal does *not* offend constitutional principles. (*People v. Fuiava, supra,* 53 Cal.4th at p. 716; *People v. Wilson* (2008) 44 Cal.4th 758, 820-821.)

The trial court has broad determination to discharge a juror who is unable to perform the duties of a juror. However, our review for an abuse of discretion requires a somewhat stronger showing than what is ordinarily implied by an abuse of discretion standard of review. The juror's inability to perform as a juror must appear in the record as a *demonstrable reality.* The record must also show that the trial court *actually relied* on this evidence. This heightened standard of review reflects our obligation to protect a criminal defendant's fundamental constitutional rights. (*People v. Fuiava, supra,* 53

[52] Childs argues that if a juror engages in misconduct, he or she may not be replaced by an alternate, but a mistrial must be granted. (*People v. Hamilton* (1963) 60 Cal.2d 105, 127.) He fails to note that the California Supreme Court later characterized this aspect of *Hamilton* as dicta and specifically disapproved it. (See *People v. Daniels* (1991) 52 Cal.3d 815, 864-866.) We address the issue Childs raises on the basis of current law.

Cal.4th at pp. 711-712; *People v. Lomax* (2010) 49 Cal.4th 530, 589-590; *People v. Wilson, supra,* 44 Cal.4th at p. 821; *People v. Barnwell, supra,* 41 Cal.4th at pp. 1052-1053; *People v. Cleveland, supra,* 25 Cal.4th at p. 474.)

"Bias is often intertwined with a failure or refusal to deliberate." (*People v. Lomax, supra,* 49 Cal.4th at p. 589.) Thus, even if there is reasonable possibility that the juror's difficulties related to his or her view of the merits of the case, the trial court still retains discretion to remove the juror for good cause. (*People v. Fuiava, supra,* 53 Cal.4th at p. 716; *People v. Thompson* (2010) 49 Cal.4th 79, 137-138 [rejecting contrary federal rule].) If it learns that there might be grounds for discharging a juror based on failure to deliberate, the trial court may conduct whatever inquiry is reasonably necessary to determine if such grounds exist. (*People v. Cleveland, supra,* 25 Cal.4th at pp. 480, 484; see *People v. Fuiava, supra,* 53 Cal.4th at p. 714 [not mandatory to conduct inquiry].)

3. *Demonstrable Reality*

Childs contends that the record does not show as a demonstrable reality that Juror No. 12 refused to deliberate or was unable to perform his duties as a juror. If the record does not demonstrate a failure to deliberate, the trial court's removal of that juror constitutes an abuse of discretion requiring reversal. (See, e.g., *People v. Cleveland, supra,* 25 Cal.4th at pp. 475, 486.) Childs reasons that the record shows that the juror was removed because he had doubts about the sufficiency of the prosecution's evidence.[53]

We disagree. The record is clear that the actual basis of the trial court's removal of Juror No. 12 was his violation of his duty as a juror not to reveal the content of

[53] Childs also assert that Juror No. 12 disagreed with the other jurors about the meaning of the jury instructions and the correct interpretation of section 502, subdivision (c)(5). As these assertions pose legal questions that we have already rejected, we need not consider them.

pending deliberations and his threat to render a non-impartial verdict. An unwillingness to perform the duties of a juror constitutes good cause for removal. (§ 1089; see, e.g., *People v. Collins* (1976) 17 Cal.3d 687, 694-697, superseded on another point in *People v. Boyette* (2002) 29 Cal.4th 381, 462, fn. 19.) A juror's willful failure to follow one instruction may lead a trial court to determine that the juror will not follow other instructions and is thus unable to perform the duties of a juror. (*People v. Ledesma* (2006) 39 Cal.4th 641, 738.) Juror No. 12's repeated threat that he might render a biased verdict if his wishes were not met, reinforced by his past refusal to follow the trial court's instructions, established good cause for removal as a demonstrable reality. (See *People v. Fuiava, supra,* 53 Cal.4th at pp. 711-712; *People v. Lomax, supra,* 49 Cal.4th at pp. 589-590.)

Childs reasons that Juror No. 12 merely committed a trivial violation of the trial court's admonition not to reveal the jury's guilt-or-innocence vote that did not require his removal. This reasoning is thrice-flawed. First, the failure to heed the trial court's instructions not to reveal the jury's deliberations was not trivial. The trial court was charged with protecting the secrecy and sanctity of the jury's deliberative process.[54] (See *People v. Fuiava, supra,* 53 Cal.4th at p. 710; *People v. Cleveland, supra,* 25 Cal.4th at p. 475; see also *People v. Wilson, supra,* 44 Cal.4th at p. 839.) Second, Childs's argument assumes that the trial court had no power to remove Juror No. 12 unless this action was required. By law, a trial court has *discretion* to discharge a juror on a showing of good cause. (§ 1089.) Even knowing that this juror was unconvinced of the sufficiency of the prosecution's evidence, the trial court retained its discretion to remove him for good cause. (See *People v. Fuiava, supra,* 53 Cal.4th at p. 716; *People v. Thompson, supra,* 49 Cal.4th at pp. 137-138.) Finally, this claim of error is a veiled attempt to reweigh the evidence before the trial court—which we may not do on appeal,

[54] We note that the trial court made significant efforts to prevent such a disclosure.

even when applying the heightened review required in juror removal cases. (See *People v. Fuiava, supra,* 53 Cal.4th at pp. 713-714; *People v. Lomax, supra,* 49 Cal.4th at p. 589; *People v. Barnwell, supra,* 41 Cal.4th at pp.1052-1053.)[55]

In the case before us, Juror No. 12 committed serious and willful misconduct, which constitutes good cause to find that the juror is unable to perform his or her duties. Such misconduct raises a presumption of prejudice which—if not rebutted—will nullify the verdict. We are satisfied that Juror No. 12 was actually removed from the jury for good cause which appears in the record as a demonstrable reality.

E. *Sufficiency of Evidence*

In his final attack on his conviction, Childs contends that the evidence was insufficient to prove that he violated subdivision (c)(5) of section 502 and must be reversed. Arguing that the unauthorized access of a hacker is an implied requirement of this offense, he reasons that his conduct did not violate that provision as a matter of law and thus, his conviction deprived him of due process. In effect, Childs challenges the trial court's legal conclusion about the meaning of the statute under which he was

---

[55] Childs asserts that Juror No. 12 never made a "threat" to hold the court "hostage." He did not raise this challenge in his opening brief. Raising an issue for the first time on appeal in a reply brief is unfair to the People, who have no opportunity to respond to it. (*People v. Zamudio, supra,* 43 Cal.4th at pp. 353-354; see *Varjabedian v. City of Madera, supra,* 20 Cal.3d at p. 295, fn. 11; see also 9 Witkin, Cal. Procedure, *supra,* Appeal, § 723, pp. 790-791.) If the issue was properly before us, we would reject it. Such clear language is not required. Jurors may have difficulty articulating their concerns in a manner that protects the confidentiality of deliberations and gives the trial court accurate information about why deliberations are stalled. (*People v. Engelman, supra,* 28 Cal.4th at p. 446.) The trial court was entitled to assess Juror No. 12's credibility, and we defer to this factual determination on appeal. (See *People v. Lomax, supra,* 49 Cal.4th at p. 590; *People v. Barnwell, supra,* 41 Cal.4th at p. 1053; see also *People v. Bennett* (2009) 45 Cal.4th 577, 621.)

Childs also argues in his reply brief for the first time on appeal that Juror No. 12 asked for an accommodation based on his physical disability. The juror's own words dispute this conclusion. When asked if his request for a longer lunch break was a physical requirement, he said it was not—that it was his custom to take a nap at lunch and the shorter lunch break ordered by the trial court was insufficient to allow him to do so.

convicted. In such circumstances, we conduct an independent review of legal issue posed. (*People v. Shabazz* (1985) 175 Cal.App.3d 468, 473-474; see *Chrisman, supra*, 155 Cal.App.4th at p. 33.) We have already rejected Childs's claim that subdivision (c)(5) can never apply to an employee who abuses computer access which he was lawfully given. (See pt. II, *ante*.) We necessarily reject this aspect of his due process argument.

Childs also challenges the sufficiency of evidence to support his conviction because he contends that his refusal to disclose access codes to his employer did not cause any denial or disruption of computer services. We have rejected this underlying argument, as well. (See pt. III.A.3, *ante*.) To the extent that this sufficiency of evidence claim of error is a restatement of his earlier vagueness challenge, we reject it again.

Faced with a true sufficiency of evidence challenge, the test is not whether the evidence supports the verdict beyond a reasonable doubt. (*People v. Johnson* (1980) 26 Cal.3d 557, 576.) Instead, we review the whole record in the light most favorable to the jury's verdict to determine if it contains substantial evidence—evidence that is reasonable, credible, and of solid value—from which a reasonable trier of fact could find the defendant guilty beyond a reasonable doubt. (*People v. Smith* (2005) 37 Cal.4th 733, 738-739; *People v. Snow* (2003) 30 Cal.4th 43, 66; *People v. Johnson*, *supra*, 26 Cal.3d at pp. 576-577.) We are not limited to the slice of evidence that Childs offers, nor to his interpretation of his conduct. We must presume in support of the judgment every fact that the jury could reasonably deduce from the evidence. (*People v. Smith, supra,* 37 Cal.4th at p. 739.) The jurors are the sole arbiters of the credibility of witnesses and the testimony of a single witness is sufficient to support a verdict. (*People v. Watts* (1999) 76 Cal.App.4th 1250, 1258-1259.) Applying this standard, the record is clear that by his conduct, Childs knowingly disrupted or denied computer services to lawful users of the City and County of San Francisco's FiberWAN network. (See pt. III.A.3, *ante*.)

IV. ENHANCEMENT

A. *Taking*

Childs also raises two challenges to the jury's enhancement finding. In the first, he argues that we must strike the section 12022.6 enhancement as there was no taking as a matter of law. When one "takes, damages, or destroys any property" in the commission of a felony with the intent to cause that result, the trial court must impose an enhancement term. If the loss exceeds $200,000, a consecutive term of two years must be added to the punishment prescribed for the underlying felony. (§ 12022.6, subd. (a)(2).) The jury found the enhancement allegation to be true. A motion for new trial challenging the enhancement was rejected and Childs received a two-year term based on this finding.

In part, Childs's argument on appeal is related to his claim that his conduct did not result in any denial or disruption of computer services. To the extent that this enhancement challenge is grounded in the same reasoning, we reject it for reasons we have already explained. (See pt. III.A.3., *ante*.) He also asserts that because no case has ever applied this enhancement to a section 502 computer crime, the Legislature could not have intended that a section 502 violation should support a section 12022.6 enhancement. He ignores the fact that the enhancement statute specifically makes it applicable to "property taken, damaged, or destroyed in violation of section 502"—the very offense of which he was convicted. (§ 12022.6, subd. (d); see *People v. Beaver* (2010) 186 Cal.App.4th 107, 118 [by its clear terms, § 12022.6 is not limited to theft offenses]; *People v. Superior Court (Kizer)* (1984) 155 Cal.App.3d 932, 935-936.)

Next, Childs urges us to conclude that this enhancement does not apply because it is unclear whether the loss that DTIS suffered as a result of his conduct constituted a "taking" within the meaning of section 12022.6, subdivision (a). He reasons that this is a statutory ambiguity requiring that section 12022.6 be construed in his favor. If a penal statute is capable of more than one reasonable construction, we ordinarily adopt the construction most favorable to the defendant. (*People v. Avery* (2002) 27 Cal.4th 49, 57; *People v. Garcia* (1999) 21 Cal.4th 1, 10-11; *People v. Beaver*, *supra*, 186 Cal.App.4th at

p. 117.) However, this "rule of lenity" applies only if other means of resolving a statute's underlying ambiguity in a convincing manner are impractical. A rule of construction is not a straightjacket to be followed blindly without regard to other factors that may give a clue to the Legislature's intent. (*People v. Beaver, supra,* 186 Cal.App.4th at p. 117; see § 4 [construction of penal statutes]; *People v. Avery, supra,* 27 Cal.4th at p. 58 [requiring " 'egregious ambiguity and uncertainty' " before rule of lenity is applied].)

Relevant case law gives us a window into the legislative intent behind section 12022.6. While an earlier version of the statute required a taking or property damage to be an element of the underlying crime, it has since been broadened to apply when a sizable loss occurs in the commission of *any* felony. (*People v. Superior Court (Kizer), supra,* 155 Cal.App.3d at pp. 935-936; *People v. Kellett* (1982) 134 Cal.App.3d 949, 958; see § 12022.6, subd. (a).) The purpose of the enhancement is to deter large-scale crime—a purpose consistent with its application to Childs's case. (See *People v. Loera* (1984) 159 Cal.App.3d 992, 1002; *People v. Hughes* (1980) 112 Cal.App.3d 452, 459; *People v. Ramirez* (1980) 109 Cal.App.3d 529, 539.) Although the Legislature did not intend for the application of section 12022.6 to turn on fortuitous circumstances, even a temporary taking suffices if the loss naturally flowed from the defendant's conduct. The defendant is not entitled to a reduction for later recovered amounts. (*People v. Beaver, supra,* 186 Cal.App.4th at p. 118; *People v. Loera, supra,* 159 Cal.App.3d at p. 1002; *People v. Swanson* (1983) 142 Cal.App.3d 104, 106-109; *People v. Kellett, supra,* 134 Cal.App.3d at p. 959; *People v. Ramirez, supra,* 109 Cal.App.3d at pp. 539-540; *People v. Bates* (1980) 113 Cal.App.3d 481, 483-484.)

These cases satisfy us that the Legislature intended that we give a broad construction to "taking" within the meaning of section 12022.6. (See, e.g., *People v. Beaver, supra,* 186 Cal.App.4th at pp. 117-118 [legal expenses incurred to reduce employer's exposure to medical expenses come within § 12022.6].) In the case before us, the prosecution offered evidence that as a result of Childs's conduct the city incurred far more than $200,000 in expenses during the critical July 9 to July 21 period. (See, e.g., *People v. Swanson, supra,* 142 Cal.App.3d at pp. 106-109 [fair market value is value

of loss].) Thus, we conclude that there was substantial evidence in support of the jury's enhancement finding.[56]

B. *Defense Evidence*

Childs also contends that the enhancement finding must be reversed because the trial court prevented him from presenting a valid defense to the enhancement. He asserts that subdivision (e)(1) of section 502 required the city to seek injunctive relief against him, that it did not do so, and that its expenditure of large amounts of money to hire outside experts to regain administrative control of the FiberWAN network was unreasonable without first attempting to pursue civil remedies. (§ 12022.6; see § 502, subd. (e)(1).) In the trial court, during the motion in limine phase of the case, Childs sought to introduce expert testimony that the city was unreasonable when it failed to bring an injunctive action against him. The trial court denied the motion. On appeal, he argues that this exclusion of evidence precluded him from putting on a defense to the enhancement allegation, rendering the resulting finding a violation of his constitutional rights to due process and a fair trial.

Contrary to Childs's reasoning, subdivision (e)(1) did not require the city to seek civil remedies before bringing a criminal action against him. We have already rejected this tortured statutory interpretation. That provision *allows* the victim of computer crime—which in this case happens to be the city's DTIS[57]—to take such an action. It does not *mandate* that a civil action be brought. (§ 502, subd. (e)(1); see pt. II.A., *ante*.)

The evidence that Childs offered was properly excluded because it was inadmissible. Relevant evidence tending to prove a disputed *fact* is admissible. (Evid.

---

[56] The Attorney General also argues that by copyrighting the city's FiberWAN network, Childs took it within the meaning of the statute. As we find ample other evidence to support the section 12022.6 finding, we need not address this issue.

[57] Childs's interpretation would only seem to apply if the victim of the computer crime and the county bringing the criminal prosecution were the same entity, as they are in the unique circumstances of the combined City and County of San Francisco. In most other cases, this interpretation of the intent to the statute would require the prosecution to sit idle while the victim sought civil restitution—an absurd result. (See *People v. Superior Court (Mouchaourab)* (2000) 78 Cal.App.4th 403, 428.)

Code, §§ 210, 350.) The proffered evidence was not about a factual matter on which expert testimony might be relevant. Instead, it was intended to inform the jury of Childs's *legal* interpretation of section 502, subdivision (e)(1). Courts may not allow experts to offer legal conclusions disguised as opinion testimony. An expert's opinion on an issue of law is not admissible to challenge the trial court's interpretation of legal principles to be conveyed in the jury instructions. (*Amtower v. Photon Dynamics, Inc.* (2008) 158 Cal.App.4th 1582, 1599; *Benavidez v. San Jose Police Dept.* (1999) 71 Cal.App.4th 853, 864-865; *Summers v. A. L. Gilbert Co.* (1999) 69 Cal.App.4th 1155, 1178-1179.) The jury must follow the legal principles that the trial court provides in the instructions. (*Amtower v. Photon Dynamics, Inc., supra,* 158 Cal.App.4th at p. 1599.) As the proffered expert testimony was properly excluded as irrelevant, Childs was not deprived of a defense to the alleged enhancement. (See *Amtower v. Photon Dynamics, Inc., supra,* 158 Cal.App.4th at p. 1599; *Benavidez v. San Jose Police Dept., supra,* 71 Cal.App.4th at p. 865; see also Evid. Code, §§ 210, 350.) Thus, we affirm Childs's conviction, including the enhancement finding.

V. RESTITUTION ORDER

A. *Proximate Cause*

1. *Trial Court Ruling*

In a second appeal, Childs raises two challenges to the trial court's order that he pay $1,485,790.31 in restitution. He first argues that the restitution order improperly included $1,105,929.31 in reimbursement for expenses that he reasons were not the result of his criminal conduct. He asks us to reduce the total restitution order to $379,861.[58]

A crime victim who incurs *any* economic loss as the result of the commission of a crime is entitled to restitution from the defendant. (§ 1202.4, subd. (a)(1).) When a victim suffers an economic loss *as a result* of the defendant's conduct, the trial court *must* order that the defendant make full restitution to the victim. (*Id.*, subd. (f); *People v. Giordano* (2007) 42 Cal.4th 644, 664; *People v. Harvest* (2000) 84 Cal.App.4th 641, 647,

[58] As permitted by statute, the trial court applied the $10,744 seized from Childs at his arrest to the total sum owed. (§ 1202.4, subd. (f).)

disapproved on another point in *People v. Giordano, supra,* 42 Cal.4th at p. 666, fn. 8.) To the extent possible, the restitution order must be of a dollar amount that is sufficient to fully reimburse the victim for every determined economic loss incurred as a result of the defendant's criminal conduct. (§ 1202.4, subd. (f)(3); *People v. Gemelli* (2008) 161 Cal.App.4th 1539, 1542.) The right to restitution is grounded in our state constitution. (See Cal. Const., art. I, § 28, subd. (b)(13); *People v. Keichler* (2005) 129 Cal.App.4th 1039, 1045.)

DTIS—as the party seeking restitution—bore the burden of providing an adequate factual basis for its claim. (See *People v. Giordano, supra*, 42 Cal.4th at pp. 664, 667; see also § 1202.4, subd. (f).) The trial court heard evidence that expenditures after DTIS regained access to the FiberWAN were reasonably related to Childs's failure to provide access from July 9 to July 21. The lockout convinced DTIS officials that an assessment of the network configurations was necessary to maintain the integrity of the FiberWAN network for the city's departments. Some of the information in the city's computer system was sensitive and personal. DTIS and its outside vendors reviewed the configurations of firewalls and other security devices to which Childs had had access, in part to make sure that he—and other possible intruders—did not have access to the FiberWAN from an outside source. DTIS sought to ensure that there would be no further disruptions of the FiberWAN network. A prima facie case was offered that $1,105,929.31 was spent to monitor and respond to security threats that came to light after Childs locked DTIS officials out of the computer system.

Once the victim makes a prima facie showing of economic loss incurred as a result of the defendant's criminal acts, the burden of proof shifts to the defendant to discredit those amounts. (*People v. Gemelli, supra,* 161 Cal.App.4th at p. 1543.) Childs challenged the scope of the restitution order that the prosecution sought. He conceded that DTIS was entitled to reimbursement for $379,861 spent attempting to regain administrative control of the FiberWAN system from July 9—when he refused to provide administrative access to Robinson—until July 21 when he provided that information to Mayor Newsom. However, he argued that $1,105,929.31 in costs incurred *after* he

provided DTIS with access to the FiberWAN system could not be lawfully attributed to his conduct. Childs reasoned that if he had provided administrative access to the FiberWAN system and resigned from city service, these costs would still have been incurred. As such, he argued, the later-incurred costs were not attributable to his criminal conduct.

The trial court reasoned that the purpose of restitution was to make the victim whole. It ruled that DTIS's expenses to insure the integrity of the network after Childs's denial of access did result from his criminal conduct. It included the disputed $1.1 million in the restitution order to reimburse DTIS for the cost to install a new city-wide security system and to investigate whether Childs continued to have access to information stored in FiberWAN databases after his suspension.

2. *Ongoing Security and Access Issues*

On appeal, Childs again concedes that the $379,861 that DTIS spent during the July 9-21 period to attempt to regain administrative access to the FiberWAN network was properly included in the restitution order. However, he continues to challenge the trial court's conclusion that he was also required to reimburse DTIS for $1,105.929.31 spent to install a new city-wide security system and to determine if he improperly accessed the databases of city departments to view information stored there. He argues that these sums were not proximately caused by his denial or disruption of the FiberWAN network to an authorized user. Instead, he reasons that these funds were spent to upgrade the city's computer security systems and to investigate the possibility that Childs had engaged in conduct which there was no proximate cause to believe that he had done. He urges us to conclude that $1.1 million dollars of DTIS's expenditures were too remote and too unrelated to his criminal conduct to be properly included in the restitution order.

The right of restitution is to be broadly and liberally construed. (*People v. Keichler, supra,* 129 Cal.App.4th at p. 1045; see § 1202.4, subd. (f)(3) [making non-exclusive list of types of economic losses].) A restitution award is committed to the sound discretion of the trial court, guided by the factors pertaining to the particular claim. (*People v. Giordano, supra,* 42 Cal.4th at p. 665.) The restitution order is determined

based on proof by preponderance of evidence, not proof beyond a reasonable doubt. (*People v. Gemelli, supra,* 161 Cal.App.4th at p. 1542; *People v. Keichler, supra,* 129 Cal.App.4th at p. 1045.) On appeal, we review the restitution order for an abuse of that discretion.[59] To warrant reversal, the order must be arbitrary and capricious, by falling outside the bounds of reason under the applicable law and the relevant facts. (*People v. Giordano, supra,* 42 Cal.4th at p. 663; *People v. Gemelli, supra,* 161 Cal.App.4th at p. 1542; *People v. Maheshwari* (2003) 107 Cal.App.4th 1406, 1409.) We presume that the trial court's ruling was correct, inferring the truth of all facts supported by the record. (*People v. Giordano, supra,* 42 Cal.4th at p. 666.)

To warrant restitution, the victim's economic loss must have been incurred as a logical result of the defendant's criminal conduct. (§ 1202.4, subds. (a)(1), (f); *People v. Holmberg* (2011) 195 Cal.App.4th 1310, 1320-1321; *People v. Maheshwari, supra,* 107 Cal.App.4th at pp. 1409-1410 [investigative fees]; *People v. Lyon* (1996) 49 Cal.App.4th 1521, 1525-1526 [asset protection; not legal costs to oppose criminal defense discovery].) Courts apply tort principles of proximate cause when making this determination, weighing in those policies that limit a person's responsibility for the consequences of his or her conduct. (*People v. Holmberg, supra,* 195 Cal.App.4th at p. 1321; see *People v. Jones* (2010) 187 Cal.App.4th 418, 425-427.) Under those principles, if the defendant's conduct was a substantial rather than a theoretical factor in the victim's loss, then the loss was proximately caused by the defendant's conduct. The key inquiry is whether reasonable people would regard that conduct as a cause of the loss. (*People v. Holmberg, supra,* 195 Cal.App.4th at pp. 1321-1322.)

Childs disputes that his conduct created a security breach requiring expensive redesign and remediation work. He argues that when he was the system administrator, FiberWAN security was high, suggesting that no improved security was required after his removal. His argument ignores the obvious—that once he was no longer the system

[59] Some cases apply a substantial evidence test, but as Childs makes a legal argument—not a factual challenge—the abuse of discretion standard seems more appropriate. (See, e.g., *People v. Baker* (2005) 126 Cal.App.4th 463, 468-469.)

administrator, the risk that *Childs himself* might make what would then have become an unauthorized intrusion into the computer network was a risk that DTIS was reasonably required to assess, detect, and prevent in order to protect the integrity of the FiberWAN databases. DTIS was entitled to recover the expense of preserving the integrity of its network after Childs's criminal act highlighted the risks he posed to that network. (See, e.g., *People v. Lyon, supra,* 49 Cal.App.4th at p. 1525 [legal expenses spent to preserve victim's asset properly included in restitution order].)

Childs also argues that these expenses cannot be charged to him because there was no evidence that he actually made an unauthorized intrusion into the network. We are satisfied that DTIS was not required to wait for Childs to make such an intrusion before taking measures to protect itself. (See *People v. Mearns* (2002) 97 Cal.App.4th 493, 501-502 [sexual assault victim relocation expenses constituted economic losses for restitution]; see also § 1202.4, subd. (f)(3)(J), (L) [installation of burglar alarm and expenses to repair credit rating as losses for purposes of restitution].) Once the potential for him to make unauthorized access to the FiberWAN became known, DTIS could reasonably expend funds to prevent him from making that potential risk an actual intrusion. Those expenses are an economic loss subject to restitution.

Childs takes a narrow view of his crime, characterizing it as no more than refusing to provide administrative access to the FiberWAN network for twelve days. By contrast, courts considering the propriety of a restitution order may take a broad view of the evidence adduced at trial. (See, e.g., *People v. Holmberg, supra,* 195 Cal.App.4th at p. 1322 [receiving stolen property was concurrent cause of economic loss].) There can be more than one cause of an injury and multiple causes can result in harm. (*Ibid.* [one convicted of receiving and concealing stolen property was substantial factor in victim's economic loss].) As his criminal conduct was a substantial factor in the city's economic loss, the related expenses were properly included within the trial court's restitution order. (See, e.g., *Id.* at pp. 1321-1322.)

The scope of Childs's criminal conduct is not as limited as he asserts. The evidence adduced at trial supports findings that he configured the FiberWAN network to

preclude anyone else from having access to it, made it more vulnerable to intrusion by publishing its configurations as part of his copyright application, concealed the backup configurations and created connections that might have allowed him to have unauthorized and undetected access to the system. We are satisfied that the restitution order was within the trial court's discretion. Its finding was rational, well-reasoned, based on facts presented at the hearing, and within its broad discretion. (See, e.g., *People v. Mearns, supra,* 97 Cal.App.4th at p. 502.)

B. *Excessive Fine*

Childs next asserts that the restitution order constituted an excessive fine and urges its reversal on that constitutional ground.[60] The United States and California constitutions bar the imposition of an excessive fine, either under the direct authority of the ban on such fines or the due process implications of a grossly excessive punishment. (See U.S. Const., 8th Amend.; Cal. Const., art I, § 17; *Austin v. United States* (1993) 509 U.S. 602, 607-610; *People ex rel. Lockyer v. R.J. Reynolds Tobacco Co.* (2005) 37 Cal.4th 707, 727-728.) A civil penalty may violate these constitutional provisions. (See, e.g., *People ex rel. Lockyer v. R.J. Reynolds Tobacco Co., supra,*37Cal.4th at pp. 726-731.)

The principle of proportionality guides our inquiry into the constitutionality of a sizable restitution order. We consider the defendant's culpability, the relationship between the harm caused and the restitution ordered, penalties imposed by similar

---

[60] Childs also argues that DTIS did not show that the actual harm suffered by the city was the equivalent of the amount of restitution ordered. This claim of error suffers from two flaws. First, he made no such argument in the trial court, as he was obliged to do. (See *People v. Gemelli*, *supra,* 161 Cal.App.4th at p. 1543; *People v. O'Neal* (2004) 122 Cal.App.4th 817, 820.) Thus, he may have waived this issue by not raising it in the trial court. Even if the argument was properly before us, it is without merit. The cases he cites in support of this claim of error turn on whether a restitution order should be based on the amount charged by a medical provider or the lesser amount actually paid by an insurer. (See *In re Anthony M.* (2007) 156 Cal.App.4th 1010, 1013, 1018-1019; *People v. Hove* (1999) 76 Cal.App.4th 1266, 1274-1275.) As there was no evidence challenging DTIS's ample evidence that it actually paid its employees and vendors the claimed amounts, these cases do not bear on our analysis.

statutes, and the defendant's ability to pay. (*People ex rel. Lockyer v. R.J. Reynolds Tobacco Co., supra,* 37 Cal.4th at p. 728; see *United States v. Bajakajian* (1998) 524 U.S. 321, 334, 337-338, superseded on another point as stated in *U.S. v. Del Toro-Barboza* (9th Cir. 2012) 673 F.3d 1136, 1154.)

Childs argues that the $1.5 million restitution ordered was disproportionate to the gravity of his offense. A trial court has broad discretion to determine the amount of a restitution order. The key inquiry is whether the amount of the forfeiture bears some relationship to the gravity of the offense it is intended to punish. (*People v. Urbano* (2005) 128 Cal.App.4th 396, 406.) In making this argument, Childs again minimizes his conduct. (See pt. V.A.2., *ante*.) The record establishes that he knowingly prevented the city from being able to use its own computer system for a period of time, deliberately configured that system so that no one else could access it, set it up so that anyone other than him attempting to enter it would erase the data stored in it, and made the network more vulnerable to external attack by the filing of an unauthorized copyright application. This evidence justifies the restitution amount ordered. (See, e.g., *Id.* at p. 406.)

He also claims that this penalty is not comparable to that imposed for more serious, violent offenses. The Legislature commands restitution be given for *economic* losses. (§ 1202.4, subd. (a)(1); see *People v. Harvest, supra,* 84 Cal.App.4th at p. 647.) The suffering inflicted as a result of being the victim of a violent offense is not compensable under this provision. It is not comparable to the economic loss resulting from a computer crime. As the violent and nonviolent offenses are of different classes, those offenses are not sufficiently similar to make this comparison persuasive.

Childs also claims that he has no ability to pay this sum. Even if he had offered evidence to support this assertion in the trial court, the other factors in our analysis would outweigh this concern. Considering all the proportionality factors, we are satisfied that the trial court's restitution order was set in an amount that did not constitute an excessive fine.

C. *Criminal or Civil Order*

Finally, Childs contends that the restitution order was punitive in nature and thus violated his federal and state constitutional rights to due process and to a jury trial. He complains that after DTIS's prima facie evidence of loss, the burden of proof shifted to him to rebut that evidence. He also objects that the order was grounded in facts found by the trial court by a mere preponderance of evidence. Childs reasons that he had a right to a jury trial on the facts necessary to impose this fine and that those facts had to be found beyond a reasonable doubt. He asks us to set aside the trial court's restitution order and remand the case for a jury determination of restitution. (See U.S. Const., 6th & 14th Amends.)[61]

Courts have held that due process does not require that a restitution hearing be conducted with all of the formalities of a criminal prosecution. (*People v. Giordano, supra,* 42 Cal.4th at p. 662 fn. 6; *People v. Harvest, supra,* 84 Cal.App.4th at pp. 647-650; *People v. Hove, supra,* 76 Cal.App.4th at p. 1275; see *People v. Gemelli, supra,* 161 Cal.App.4th at p. 1542; *People v. Keichler, supra,* 129 Cal.App.4th at p. 1045.) In 2007, the California Supreme Court noted that this court-approved practice had evolved before more recent United States Supreme Court and California Supreme Court decisions establishing that the right to jury trial requires that a jury determine by proof beyond a reasonable doubt any fact that exposes a defendant to a greater sentence. As the issue was not raised in that case, the California Supreme Court did no more than note that it might be an issue in a future case. (*People v. Giordano, supra,* 42 Cal.4th at pp. 662, fn. 6; see *Cunningham v. California* (2007) 549 U.S. 270, 281; *People v. Black* (2007) 41 Cal.4th 799, 809.) Childs construes this language to require that the restitution issue be determined by a jury.

Subsequent case law does not support this contention. Since the California Supreme Court decision in *Giordano,* the United States Supreme Court has ruled that the

---

[61] Childs acknowledges that he did not object in the trial court on these grounds. However, these due process and jury trial issues may be considered on appeal, despite the lack of objection. (*People v. French* (2008) 43 Cal.4th 36, 46; *People v. Partida* (2005) 37 Cal.4th 428, 435-436.)

Sixth Amendment does not require a jury determination about whether to impose consecutive or concurrent terms. That issue may be resolved by the trial court alone. (*Oregon v. Ice* (2009) 555 U.S. 160, 163-164.) The determination of restitution fines was specifically cited as another example of issues that the high court opined could properly be determined by the trial court without a jury finding. (*Id.* at p. 171-172.)[62]

Childs's assumption fares no better when we consider more recent California appellate court decisions. The California Supreme Court has yet to rule on the issue, but appellate courts have rejected the defendant's claim that section 1202.4 restitution constitutes an increased punishment for crime, thus rejecting a necessary predicate to implicate the Sixth Amendment right to jury trial. (*People v. Chappelone* (2010) 183 Cal.App.4th 1159, 1184 [citing many federal cases consistent with its ruling]; *People v. Millard* (2009) 175 Cal.App.4th 7, 35-36; see *People v Wilen* (2008) 165 Cal.App.4th 270, 288-289.) We are satisfied that the trial court's restitution order was properly entered, without the need for a jury determination or proof beyond a reasonable doubt. (See *People v. Millard, supra*, 175 Cal.App.4th at p. 36.)

The judgment of conviction and the restitution order are affirmed.

[62] Childs criticizes any reliance on this decision, as it commanded only five votes and engendered a vigorous dissent. A 5-4 decision of the United States Supreme Court is a majority decision that is binding on us.

_____
REARDON, J.

We concur:

_____
RUVOLO, P. J.

_____
RIVERA, J.

Trial Court:	San Francisco Superior Court
Trial Judge:	Hon. Teri L. Jackson
Counsel for Appellant:	Philip M. Brooks By appointment of the Court of Appeal pursuant to the Independent Case System First District Appellate Project
Counsel for Respondents:	Kamala D. Harris Attorney General of California Dane R. Gillette Chief Assistant Attorney General Gerald A. Engler Senior Assistant Attorney General Catherine A. Rivlin Supervising Deputy Attorney General Karen Z. Bovarnick Deputy Attorney General