[Cite as *Gornes v. Dayton*, 173 Ohio App.3d 37, 2007-Ohio-4548.]

IN THE COURT OF APPEALS OF OHIO
SECOND APPELLATE DISTRICT
MONTGOMERY COUNTY

GORNES,	:	
	:	Appellate Case No. 22065
Appellant,	:	
	:	Trial Court Case No. 06-CV-2858
v.	:	
	:	(Civil Appeal from
THE CITY OF DAYTON,	:	Common Pleas Court)
	:	
Appellee.	:	

. . . . . .

O P I N I O N

Rendered on the 31st day of August, 2007.

. . . . . .

David M. Duwel, and Todd T. Duwel, for appellant.

Green & Green, Thomas M. Green, and Stacy M. Wall, for appellee.

. . . . . .

FAIN, Judge.

{¶ 1} Plaintiff-appellant Helen Gornes appeals from a trial court judgment affirming the decision of the city of Dayton Civil Service Board ("DCSB") to dismiss Gornes from her employment with the city of Dayton ("City"). The trial court concluded that the DCSB's decision was supported by a preponderance of substantial, reliable, and probative evidence and was not arbitrary, capricious, unreasonable, illegal, or unconstitutional.

{¶ 2} Gornes contends that the trial court's judgment is against the manifest weight of the evidence, because there is no evidence that Gornes was personally involved with the activity that led to her termination. We conclude that the trial court's judgment is supported by substantial, reliable, and probative evidence. Accordingly, the judgment of the trial court is affirmed.

{¶ 3} On cross-appeal, the City contends that the trial court erred by allowing Gornes to elect to proceed with her appeal under R.C. Chapter 2506, rather than under R.C. 119.12. Because we are affirming the decision of the trial court, the cross-appeal is moot.

I

{¶ 4} Helen Gornes was employed by the City between August 1996, and February 2005, when she was dismissed from employment after a show-cause hearing. At the time of her dismissal, Gornes was a systems engineer and was one of only three people who had administrative security clearance and access to the e-mail accounts of other users on the City's e-mail system. The other two people with clearance were Michael MacDonald and Chris Parriman. Although these three individuals had the ability to open other employees' e-mail, City policy prohibited anyone from accessing another employee's e-mail without being directed to do so by the appropriate authority or without direct permission from the employee in question.

{¶ 5} The events leading to Gornes's dismissal began in November 2004, when MacDonald sent an e-mail to Bill Hill, who was the City's Director of Information and Technology Services ("ITS"). MacDonald was upset with another ITS employee, Ken Bain,

and made uncomplimentary remarks about Bain in the e-mail. MacDonald sent the e-mail only to Hill, not to other employees. Nothing more happened with this e-mail for about a month.

{¶ 6} As was noted, Gornes was one of three systems engineers who had administrative power over all the City's computer systems. On December 1, 2004, Gornes removed administrative access from the accounts of various users who had previously been able to access other employees' e-mail. One of these accounts belonged to Scott Sizemore, who complained to Gornes and others on December 2, 2004, about the changes.

{¶ 7} December 2, 2004, was also Gornes's birthday. Gornes worked all day and then went to dinner that evening with two people from the office (Ken Bain and Penny Hamrick). At the time, Gornes was the primary engineer working on building a cluster server called the Exchange 02 server. Bain was the only other employee working on that server and was helping Gornes build the server.

{¶ 8} After having dinner and drinking a couple of pitchers of Bad Juan Margaritas,[1] Gornes went home, where her husband surprised her by being home for her birthday when he was supposed to be out of town. They continued drinking. According to Gornes, she went to bed at some point and woke up the next morning after 8:00 a.m. Gornes called the help-desk to indicate that she would be late, and then arrived at work around 9:00 a.m.

{¶ 9} In the meantime, in the early morning hours of December 3, 2004, MacDonald's e-mail account was accessed, and the e-mail from MacDonald to Hill was

[1]Referred to in the transcript as "Bad One" margaritas.

forwarded to Bain's e-mail account. The access occurred between 2:00 a.m. and 3:00 a.m. Around 4:00 a.m., Bain opened the e-mail and wrote an angry response to MacDonald. When MacDonald arrived at work on December 3, 2004, he discovered the e-mail from Bain. MacDonald realized something was wrong when he saw that the original e-mail had been forwarded to Bain from MacDonald's own account.

{¶ 10} MacDonald alerted Karen Ater, who was the most senior person present in the ITS department that day. While MacDonald was talking with Ater, another employee, Scott Sizemore, came into Ater's office. Sizemore mentioned that all of his e-mail had been deleted from the system, other than one e-mail that had been generated that morning. MacDonald, Ater, and Sizemore then went to MacDonald's office and checked the computer logs. These logs indicated that Helen Gornes had been logged in at 2:52 a.m., very close to the time that the e-mail was sent from MacDonald's account.

{¶ 11} Gornes had two accounts that had administrator privileges and that would have allowed her to access other employees' e-mail. One account was called "hgornes" and the other was called "hgadmin." The "hgornes" account was the one that was logged in at the time the e-mail was sent from MacDonald to Bain.

{¶ 12} The specific time that Sizemore's e-mail account was accessed was unknown, but it was between 1:32 a.m. and 7:56 a.m. At around 7:56 a.m., Gornes's "hgadmin" log-on and account was used to delete the audit log. This log records various events like the identity of an account that accesses a particular e-mail box and the time of access. The computer system automatically generates the audit log, and there would never be a business reason to delete it. The audit log is a security log that is in place to specifically track this type of activity, and the fact that it was deleted was suspicious.

{¶ 13} Gornes stipulated before the DCSB hearing that her log-on and password were used to access the e-mail accounts of both MacDonald and Sizemore. However, Gornes denied being the individual who used her log-on and password. She claimed that she was home asleep at the time and that someone else must have obtained her passwords.

{¶ 14} A user account is set for each City employee and is accessed by an individually assigned log-on and password. These accounts give users access only to the material or information for which the particular user has clearance. The accounts "hgornes" and "hgadmin" were "domain administrator accounts" that had unrestricted access to all domain resources for the City. In addition, both accounts had full administrative privileges for the Exchange database, which was the computer server for e-mail.

{¶ 15} The City maintained (and Gornes had no information to suggest otherwise) that all access of the hgornes and hgadmin accounts on December 3, 2004, was done remotely, off the City's premises. The City's computer system was designed so that users could access it remotely, from other locations, through a server called CODMFS14 and using a connection protocol called "ICA." "COD" stands for "City of Dayton" and "MFS" stands for "MetaFrame Server."

{¶ 16} Connection protocols like "http" or "ICA" are equivalent to a language and allow two different computer systems to communicate with each other based on this common language. The remote connection to the City's MetaFrame Server could be done over the Internet or via dial-up servers.

{¶ 17} Gornes testified that she owned a Dell personal computer, not a laptop, and

that her internet provider was Time-Warner. Therefore, Gornes claimed that if she had tried to remotely access the City's computers, she would have used her Roadrunner account, which she had with Time Warner.

{¶ 18} Each Internet provider like Time Warner, SBC, GTE, and so forth, owns a range of Internet Provider ("IP") addresses. The provider assigns an IP address to each user account that logs onto the Internet, but different things can cause the IP address to change. If the individual user reboots his or her system, the IP address can change. In addition, the provider may assign the number for only a limited period of time. In Time Warner's case, the duration of an assignment is normally anywhere from one to seven days.

{¶ 19} An IP address is similar to a telephone number, which can identify a caller. However, the City cannot determine the identity of the individual to whom a specific IP address has been assigned because that information is contained in a separate system -- the records of the Internet provider.

{¶ 20} When an outside computer attempts to remotely access CODMFS14, it must first pass through a firewall, a remote-access server, and another firewall, which all sit between the City and the Internet. The firewall is set up to monitor and secure outside connections from coming into the City's computer system unless the connections are properly authenticated. If an attempt is made to come into the City's system, the IP address will be caught or reflected in one of the firewall blocks. These attempts are logged, even if the connection or attempted log-in fails. On the night in question, the log had about 45,000 entries, but that does not mean that there were 45,000 IP addresses that attempted to connect to the City. Some of the addresses were duplicates.

{¶ 21} Neither the City nor Gornes was able to establish Gornes's Roadrunner IP address, as of December 3, 2004, because Time Warner does not keep those records long. Gornes's expert examined the IP addresses that were used on the night in question and was unable to find any Roadrunner residential IP address that accessed the system both before and after 4:00 a.m. to 4:30 a.m. This fact was allegedly significant because Gornes had a Roadrunner residential account and because the City rebooted its system every morning between 4:00 a.m. and 4:30 a.m. All users on the City's system at the time would have been kicked off and would have had to log back in to access the system. Therefore, if Gornes had been accessing the City's system from her home computer, there should have been attempts by two identical IP addresses from a Roadrunner residential account – one before the system was rebooted, and one after. This is because the e-mail accounts were accessed before 4:00 a.m. with the "hgornes" account. The "hgadmin" account was subsequently used to delete the security or audit log after 4:30 a.m. Two log-ins from Gornes's home computer would, therefore, have been required.

{¶ 22} Dayton's expert testified that when an individual subscribes to Roadrunner, he or she is given the rights to the network. Each time an individual connects to the Internet, he or she is assigned an IP address as of that moment in time. If the individual restarts the computer or loses his Internet connection, a different number will more than likely be assigned. According to the same expert, an individual could possibly be assigned the same number for 48 or 72 hours. The assignment of numbers is strictly a random process. Finally, Dayton's expert testified that there is no way to distinguish between the IP addresses of Roadrunner commercial and residential accounts.

{¶ 23} After hearing from MacDonald, Gornes, and an expert for each side, and

after considering the documentary and stipulated evidence, the DCSB found that Gornes had violated City policy and ITS department procedures by accessing another employee's e-mail without being directed to do so by the appropriate authority. DCSB concluded that discharge was appropriate because Gornes held a position of significant confidence, such that only two other City employees had the same power to access proprietary information as well as all computer records of City employees. The trial court agreed with the DCSB and affirmed the dismissal. From this adverse judgment, Gornes appeals.

II

{¶ 24} Gornes's sole assignment of error is as follows:

{¶ 25} "The trial court's decision was against the manifest weight of the evidence."

{¶ 26} Under this assignment of error, Gornes contends that the trial court decision was devoid of sound reasoning and against the weight of the evidence because the City failed to prove that Gornes's home computer accessed the City's computer system on December 3, 2004. Gornes argues that it is undisputed that she had only one personal computer and that she was home at the time the City's computer system was accessed. Gornes, therefore, contends that the City's failure to prove that any Time Warner Roadrunner IP address initially accessed the City's computer system between 2:00 a.m. and 3:00 a.m., and then later accessed the system between 4:15 a.m. and 7:56 a.m., is fatal to its claims.

{¶ 27} With regard to administrative appeals under R.C. Chapter 2506, a trial court may find "that the order, adjudication, or decision is unconstitutional, illegal, arbitrary, capricious, unreasonable, or unsupported by the preponderance of substantial, reliable,

and probative evidence on the whole record. Consistent with its findings, the court may affirm, reverse, vacate, or modify the order, adjudication, or decision, or remand the cause to the officer or body appealed from with instructions to enter an order, adjudication, or decision consistent with the findings or opinion of the court." R.C. 2506.04.

{¶ 28} The common pleas court must affirm the agency's decision, however, if the decision "is supported by a preponderance of reliable, probative, and substantial evidence." *Snyder v. Beavercreek Twp.*, Greene App. No. 2005-CA-53, 2006-Ohio-1612, at ¶ 24.

{¶ 29} Our own review is more limited. We must decide "whether the common pleas court properly applied the standard of review set forth in R.C. 2506.04. Our determination is limited to the issue of whether, as a matter of law, a preponderance of reliable, probative and substantial evidence exists to support the decision * * *, so that the common pleas court did not abuse its discretion in sustaining the * * * decision." Id. at ¶ 25, citing *Budd Co. v. Mercer* (1984), 14 Ohio App.3d 269, 273-274, 471 N.E.2d 151. We must affirm the trial court unless we find that the decision is " 'not supported by a preponderance of reliable, probative and substantial evidence.' " *Smith v. Granville Twp. Bd. of Trustees* (1998), 81 Ohio St.3d 608, 613, 693 N.E.2d 219.

{¶ 30} Based upon our review of the record, we conclude that the trial court's decision is supported by a preponderance of reliable, probative, and substantial evidence. As a preliminary point, we note that the City did not have to prove Gornes's alleged residential IP address, nor was the City required to prove that the same IP address accessed the system both before and after the system was rebooted during the early morning hours. Dayton's expert testified that IP addresses are dynamic and do not remain

the same. For example, an IP address can change if an individual restarts his or her own computer. Consequently, there was no guarantee that Gornes's IP address was, in fact, the same before and after the City's system was rebooted. Since Gornes was an experienced systems engineer, she could have been familiar with the subject of IP addresses and how they are assigned. Gornes was also aware that the City's system was rebooted in the early morning hours. Gornes, therefore, could have logged off the City's system and restarted her own computer, causing her IP address to change. In this situation, there may not have been two identical IP addresses that accessed the City's system, one before and one after the 4:00 a.m. to 4:30 a.m. time frame. Instead, two different IP addresses may have been associated with the same computer.

{¶ 31} Even if Gornes was not aware of the fact that IP addresses can change, she may simply have shut her computer down after retiring for the night, and then restarted it in the morning, as many people do. Again, in this situation, the IP addresses may not have been the same. As a result, we find no relevance in the fact the City failed to "prove" that a particular Time Warner address accessed the system both before and after it was rebooted.

{¶ 32} More importantly, Gornes's theory rests on acceptance of her credibility by the DCSB and trial court. But the DCSB was not required to believe Gornes. *Snyder*, 2006-Ohio-1612, at ¶ 28 (credibility issues are left to the trier of fact). Gornes testified that she was at home all night, had only one home computer, and had a Time Warner Roadrunner account. The trier of fact did not have to believe any of this testimony. For all anyone knows, Gornes could have had more than one computer and more than one point of access to the Internet. Gornes could have left home that evening and used other points

of access. The trier of fact did not have to believe that Gornes was home all evening, and the City was not required to prove the contrary.

{¶ 33} There is also no documentation about the Time Warner account in the record. Gornes did not submit a bill from Time Warner for the period in question. Gornes argues that no one questioned the fact that she had a Time Warner Roadrunner account. However, no one was required to question it.

{¶ 34} The City established, both through testimony and Gornes's own stipulations, that Gornes's user accounts were responsible for the invasion of the e-mail accounts on the City's system and for the deletion of the audit record that would have shown exactly what actions those accounts took, and when. The City's internal and External Electronic Communications Policy, Code 2.14, Section IX., provides, "At no time should any user access files or information other than their own private directories or files that have been identified as publicly available." The policy also states that inappropriate use of the City's Internet connection and e-mail system includes:

{¶ 35} "E. Unauthorized use of passwords to gain access to another user's information and communications.

{¶ 36} "F. Using City communications systems for electronic snooping, that is, to satisfy idle curiosity about the affairs of others, with no business reason for obtaining access to the files or communications. This prohibition applies to all users, including City communications system administrators and supervisors." Id. at 2.14, Section XII.

{¶ 37} The disciplinary actions authorized for violations of this policy include discharge. Gornes did not deny that her accounts were used to violate City policy, but attempted to explain how it could have happened without her involvement. However, her

explanations were not logical.

{¶ 38} The only other two individuals who had administrator privileges were Parriman and MacDonald. Parriman was out of town on a hunting trip at the time and did not access the City's system while he was on vacation. In addition, there has been no suggestion that Parriman was involved in any way. Gornes has suggested that MacDonald was the culprit, but it is unlikely that MacDonald would send his own insulting e-mail to the person he had insulted, a month after having written the e-mail.

{¶ 39} One is left, therefore, with the theory that some unknown person managed to steal Gornes's password, and was also knowledgeable enough about the system to know how to access other people's e-mail accounts. This unknown person must also have been very knowledgeable about computer systems because he or she knew to delete an audit log that would show the time and source of the actions that had occurred. And finally, this unknown person chose to send only one e-mail from one person's account and to delete other e-mails from another person's account. Ironically, the accounts that were violated belonged to individuals who had either criticized a friend of Gornes's or who had recently been involved in a dispute with Gornes – not with some unknown person and not even with some other known person who was identified at the hearing. In short, Gornes's "theory" does not logically add up.

{¶ 40} Furthermore, Gornes testified that she took a City laptop home on December 9, 2004, so that she could log in to the City's server for work purposes. Gornes admitted that she had taken a City laptop home in the past, meaning that she could have had a City laptop with her on the night of December 3, 2004. In addition, Gornes may have accessed the Internet the night of December 3, 2004, through Internet connections other than her

own residential Roadrunner account. Friends, neighbors, and commercial establishments have Internet accounts and connections that can be accessed by others – and the IP addresses would have been different from the IP address on Gornes's Roadrunner account.

{¶ 41} The point is not whether Gornes had only one computer, stayed home all night, or had only one Internet account; the point is that the City was not required to prove or disprove these matters in order to justify the termination. The City introduced substantial, reliable, and probative evidence from which a reasonable fact-finder could find that Gornes used her accounts in a manner that violated City and departmental policy. The City did not have to prove the precise mechanism or mechanisms Gornes employed to do so. We would also note that there were various points in the record where Gornes contradicted herself and was simply not credible, even on paper.

{¶ 42} Accordingly, because the record contains substantial, reliable, and probative evidence to support the decision of the trial court, Gornes's sole assignment of error is overruled.

III

{¶ 43} The City's sole cross-assignment of error is as follows:

{¶ 44} "The lower court erred by permitting appellant to elect her route of appeal after the filing of the city of Dayton's brief, permitting the lower court to retain jurisdiction."

{¶ 45} In view of our disposition of Gornes's sole assignment of error, the City's cross-assignment of error is moot.

IV

{¶ 46} Gornes's sole assignment of error having been overruled, the judgment of the trial court is affirmed.

Judgment affirmed.

BROGAN and DONOVAN, JJ., concur.