By Wendy Lathrop, LS, CFM

Wendy Lathrop is licensed as a Professional Land Surveyor in NJ, PA, DE, and MD, and has been involved since 1974 in surveying projects ranging from construction to boundary to environmental land use disputes. She is a Professional Planner in NJ, and a Certified Floodplain Manager through ASFPM.

The Latest "Gate"

My township taxes will probably be going up, and maybe you can gain a business lesson from my pain. Call it "Webcam-gate".

Many businesses have formal policies regarding personal activities on business time. This includes phone calls to friends, family, doctors' offices, and the bank. It also includes use of business computers to surf the web, write personal correspondence, or check private email. When such a policy does exist, it should be in writing, and there should be some formality about the employee's acknowledgment of having read it and agreed to it.

True, most of us don't like to be the overbearing bad guys in running our offices, but if we want to place limits on workers, that can't be based on assumptions that everyone behaves the way we want or expect. What is acceptable to one person may not be to another, and recognition that long distance calls cost money or that the Internet can transmit viruses is not foremost in the minds of those who need to make one quick call or check online to see if one sale is still in progress.

For any kind of company policy to be fair and enforceable, both employer and employee must enter into a formal agreement as to the subject of the policy and how it is to be applied. The practice of heaping a stack of papers into the new hire's arms while saying, "Welcome aboard" hardly offers an opportunity to review and decide whether or not to agree to abide by never-before-seen company practice. I remember working in one office that presumably allowed employees to take two personal days annually for religious reasons, but it turned out that if the holidays requested were not related to Christianity or Judaism, they were refused (and the two days were lost). In an increasingly diverse workplace, such policies hopefully have changed, but if not, job applicants should know about them before accepting a position.

The focal point for the title of this column, however, is a different kind of workplace: the classroom. My township provides a laptop to every high school student, to assure that everyone has equal access to the Internet and equal ability to turn in properly formatted assignments. There is a nominal annual insurance charge for this benefit, but that is not the issue in the lawsuit initiated in February 2010 by the family of one student. Instead, the suit claims invasion of privacy.

> **"If an employee uses a company laptop, does the employer have the right to activate a webcam at will to determine the location of the laptop at any given time?"**

The laptops students took home all had a "security feature", a webcam that could be remotely activated for individual units when the school district believed that a laptop had been lost, stolen or otherwise went missing, so that it could locate the laptop's surroundings. Students' reports or miscounts of laptops presumed to be on campus were to be the impetus for activating the "security feature". Here is where the policy issue comes into play: students did not know about the possibility of remote webcam activation. But apparently there was also no formal policy to inform the school district's technical staff of when to activate a webcam and when screen shots could be taken.

Blake Robbins was one student who apparently had not paid the requisite insurance fee, and so when the laptop assigned to him was no longer in school, the district counted it as missing or stolen. Once activated, the webcam took photos of Blake in his home, at times sleeping in his bed, at times in various states of dress or undress, at times with his family in other parts of his home. But he knew none of this until he was disciplined in school for alleged illegal behavior at home, based on a webcam image the district believed showed him with illicit pills (which Blake claims was "Mike and Ike" candy). No matter what was in his hand at the moment the laptop captured his image, it turned

continued on page 62

Lathrop, *continued from page 64*
out to be merely one of hundreds taken of him, and a fraction of about 66,000 overall webcam images snapped throughout the district.

Here is where the connection between workplace and school system comes into play. What is the extent of the rights of the employer–or school district–to protect its property? A company does have the right to check the calls reported on its monthly phone bills, which it can do in a number of ways. But is it appropriate to tap the phone on someone's desk to check if a call is work-related or personal? When it comes to computer use, parents sometimes install software that tracks each website their children visit; should employers be allowed the same privilege in relation to their employees? If an employee uses a company laptop, does the employer have the right to activate a webcam at will to determine the location of the laptop at any given time? These actions may seem preposterous in the business world, but the possibilities are there.

A second student initiated a separate lawsuit in July 2010 on the grounds of invasion of privacy. He had reported his laptop missing, a teacher found it and returned it to him, but the district kept its surveillance program active on the laptop for two additional months, taking over 1,000 photos of the student and his family in their home.

The school district has since deactivated the TheftTrack security software it had employed for several years, and has admitted that it had no official policies or procedures to activate the surveillance software. The U.S. District court ordered the district to adopt a policy relating to surveillance through students' laptops, and the school board has outright banned the district from any such webcam surveillance whatsoever. The FBI, U.S. Attorney General, and County District Attorney all pursued criminal investigations, since electronic surveillance without consent or a warrant violates Fourth Amendment Constitutional rights to privacy.

Had students known about the webcam, a piece of black electrical tape could have eliminated the problem. Meanwhile, the township's school district incurred substantial legal fees to defend its unwritten policy, and guess who pays for that mistake. But perhaps others can learn from the story and protect themselves from being hit by the "gate" swinging shut behind them.