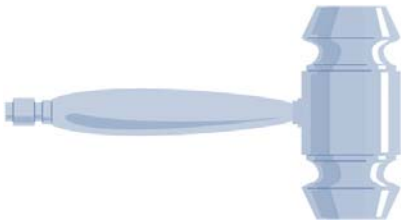
Legal Corner



By Michael I. Levin, Esq., PAESSP Chief Legal Counsel

Legal Issues in Searching Student Cell Phones: You Make the Call!

Editor's Note: Paul N. Lalley of the Levin Legal Group, P.C., contributed to this article

As a lawyer who has advised and represented school districts and school administrators in Pennsylvania for many years, I am impressed by the usually sound judgment that school principals exercise when faced with making on-the-spot decisions that have potential legal ramifications. When lawyers have a legal issue they are asked to address they typically have time to investigate the matter, research the question and prepare a (hopefully) considered response with their opinion. In contrast to the lawyer's leisurely evaluation of an issue, there often are situations where a school principal must quickly decide how to handle a problem that has potential legal consequences. These situations demand immediate action, and there is no time to contact the school district's solicitor to get advice prior to making a decision. Perhaps the principal has some familiarity with the basic legal issue involved; perhaps not. In my experience, however, school principals who acted as prudently as circumstances allow will more often than not make the correct decision from a legal perspective.

The increased use by students of more sophisticated electronic technology, however, is putting even greater pressure on school principals to make on-the-spot decisions that have legal consequences. What may the principal do if he or she believes there is evidence on a cell phone of a violation of the law or school policy, and the principal is concerned that this evidence will be lost or destroyed with the touch of a button? In these days of cell phones having functions other than simply making and receiving phone calls – such as still-photo cameras, video cameras, voicemail, Internet access and text messaging – what are the legal issues implicated where a school principal believes that a student's cell phone may contain evidence of a violation of the law or school district policy, and would like to retrieve this evidence for use in disciplinary proceedings before it is lost or destroyed? A case recently handled by my firm presents an interesting factual scenario for discussion of these legal issues.

In *Klump v. Nazareth Area School District,*[1] the school district had a policy that allowed students to carry, but not use or display, cell phones during school hours. The plaintiff in the *Klump* case was a student in the high school who got into trouble when his cell phone fell out of his pocket and came to rest on his leg. A teacher saw that the cell phone was operational — in violation of the policy — and confiscated it. The teacher and the high school's assistant principal later used the plaintiff's cell phone to call the cell phones of nine other students whose numbers were listed on the directory of the plaintiff's cell phone to see if those students were also violating school district policy. The teacher and assistant principal next accessed the text messages and voicemail stored in the plaintiff's cell phone. The teacher and the assistant principal also sent a text message from the plaintiff's phone to the plaintiff's younger brother, without identifying themselves as anyone other than the plaintiff.

What prompted the assistant principal and the teacher to check the plaintiff's text messages and voicemail and to call other student numbers from the plaintiff's cell phone? Well, the assistant principal observed a text message while in possession of the plaintiff's cell phone. This text message was from the plaintiff's girlfriend and requested an item that the assistant principal understood to be a reference to a large marijuana cigarette. Because of the contents of this text message, the assistant principal believed that the plaintiff was involved in illegal drug activity at the high school, which the assistant principal then investigated by using the plaintiff's cell phone and by accessing other text messages and voicemail messages. After learning of the school officials' use of the cell phone, the student's family filed suit against the school district, the superintendent, the assistant principal and the teacher. The lawsuit claimed that the school officials violated the student's rights under the Fourth Amendment of the United States Constitution and Article 1, Section 8, of the Pennsylvania Constitution, and that they violated Pennsylvania's Wiretapping and Electronic Surveillance Control Act (referred to as the "Wiretap Act").[2] After removing the case from state to federal court, the school district and

Continued on next page

Legal Corner - Continued from previous page

school officials moved for dismissal of the lawsuit, which the court partially granted.

Of particular interest to the issue of a school principal's accessing information from a student's cell phone is the *Klump* court's discussion of the constitutional and the Pennsylvania Wiretap Act issues. The constitutional issue arises from the protections in the Fourth Amendment and the similar – though not identical – protections in Article I, Section 8, of the Pennsylvania Constitution against unreasonable searches and seizures by government officials. School principals are government officials and are therefore subject to these constitutional limitations against unreasonable searches and seizures. Since the United States Supreme Court's landmark decision in *New Jersey v. T.L.O.*,[3] however, the courts have developed a more lenient standard for the constitutionality of searches by school officials under the Fourth Amendment than, for example, the "probable cause" standard that usually applies to searches by police officers looking for evidence of criminal activity. Under *T.L.O.*, a search by school officials will satisfy the Fourth Amendment's requirement of reasonableness if it was "justified at its inception," which means that there were "reasonable grounds for believing that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school." The Pennsylvania Supreme Court has followed the approach of *T.L.O.* in determining the reasonableness of searches and seizures by school officials under Article 1, Section 8, of the Pennsylvania Constitution, and has concluded that individualized searches of a student's possessions by school officials need to be justified only by a "reasonable suspicion" based on articulable circumstances that the student is in possession of materials that violate school rules.[4]

So how did the court in *Klump* rule on the constitutionality of the school officials' actions under these Fourth Amendment and Article I, Section 8, standards? Well, it was a mixed-bag ruling from the school district's perspective. On the one hand, the court upheld the teacher's actions in taking the plaintiff's cell phone because she directly observed the plaintiff's violation of the school district's policy prohibiting the operation of cell phones. On the other hand, the court concluded that it could not, at that early stage of the litigation, decide whether the assistant principal was justified in reviewing text messages and voicemails from the plaintiff's cell phone and in calling other students from that phone. The court could not decide those questions because the plaintiff disputed the assistant principal's claim that she observed the text message from the plaintiff's girlfriend that referred to marijuana *prior* to retrieving voicemail, searching other text messages and calling other students' numbers from the plaintiff's cell phone. This factual dispute was critically important to determining the reasonableness of the assistant principal's conduct, for purposes of the Fourth Amendment and Article 1, Section 8, of the Pennsylvania Constitution. If it eventually proved true that she observed the incriminating text message *before* undertaking her search of the cell phones text and voicemail messages, then she would have had the requisite "reasonable suspicion" to conduct those searches, and her actions would withstand constitutional scrutiny. But again, because the school officials' motion to dismiss the plaintiff's lawsuit was at the earliest procedural stage, the court had to accept as true the plaintiff's allegation that the assistant principal searched the cell phone's voicemail and text messages without a reasonable suspicion for doing so.

The other major claim in the *Klump* case points to another fact of life worth remembering: just because certain conduct may be constitutional does not mean that it is always legal. The Pennsylvania Wiretap Act issue presents a particularly difficult problem for school principals faced with evidence of a possible violation of school rules that exists on a student's cell phone. Before discussing this issue in the context of the *Klump* case, however, it is worthwhile here to provide some background on the Wiretap Act itself.

The Wiretap Act was first passed by the Pennsylvania General Assembly in 1978. It reflected the societal concerns in the mid-to-late 70s, in the immediate post-Nixon years, that government's powers to eavesdrop on telephone communications should be limited, and that people have a reasonable expectation of privacy in their telephone conversations which the law ought to protect against outside intrusion. The Wiretap Act therefore generally prohibits the surreptitious interception and disclosure of a person's "wire, electronic and oral communications" and allows a person whose communications have been illegally intercepted or disclosed to bring a lawsuit against the violator.[5] One of the more unique features of the Wiretap Act is the requirement that law enforcement

Continued on next page

Legal Corner - Continued from previous page

officers follow a specific procedure for obtaining a court order to tap a criminal suspect's phone lines, which requires the involvement of the Pennsylvania Attorney General's Office and approval from a Superior Court judge, as opposed to the usual practice of local law enforcement authorities requesting a warrant from a local county judge.[6] Another noteworthy aspect of the Wiretap Act is that a person who successfully brings a lawsuit for a violation is entitled to attorneys' fees and litigation costs, and may be able to recover punitive damages from the violator.[7] Worse still, there are criminal penalties for uses or disclosures of intercepted electronic communications: a "willful" violation is punishable as a second-degree misdemeanor. These prohibitions in the Wiretap Act explain why most school districts proceed with caution when installing security camera systems in school buildings or on school buses, and ensure that those systems record video images only, so as not to intercept oral communications that may be protected by the Wiretap Act.

So, how did the Wiretap Act come into play in the *Klump* case? The plaintiff claimed that the assistant principal violated the prohibition in section 5703 of the Wiretap Act against unlawful interception of electronic communications by accessing, and then replying to, certain text messages from the plaintiff's cell phone. The school officials countered that the plaintiff lacked legal "standing" to assert this claim because the communications that were allegedly illegally intercepted were from other people, not from him. In other words, the school officials argued that if any injury occurred by the assistant principal's alleged violation of the law, it occurred to those who sent the text messages to the plaintiff, not to the plaintiff himself. The court in *Klump* ruled in the school officials' favor on this rather technical legal issue, finding that any claim for a violation of the Wiretap Act for unlawfully intercepting text messages "belongs to the person with whom the communication originated, not the recipient." Although the school officials prevailed on this claim, the fact that the court's decision rested on the narrow ground that the plaintiff lacked legal standing to assert a Wiretap Act claim leaves the larger question still unsettled: did the school principal act illegally under the Wiretap Act in accessing the cell phone's text messages?

The contention that school officials unlawfully "intercepted" an electronic communication was not the only Wiretap Act claim asserted in the *Klump* case. The plaintiff also argued that the school officials violated section 5741 of the Wiretap Act, which prohibits unauthorized access to stored electronic communications. Specifically, section 5741 makes it unlawful to "obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage by intentionally: **(1)** accessing without authorization a facility through which an electronic communication service is provided; or, **(2)** exceeding the scope of one's authorization to access the facility."[8] The plaintiff asserted that the assistant principal's actions in pulling up and viewing stored text messages, stored phone numbers and call records from the plaintiff's cell phone violated section 5741 of the Wiretap Act.

This claim illustrates a classic problem where the law fails to keep pace with developments in technology. Rotary-dial telephones were the norm when the Pennsylvania legislature passed the Wiretap Act in the late 70s. The advent of digital and other cell phone technology, however, has made some of the definitions in the Wiretap Act obsolete. In the *Klump* case, the school officials argued that it could not constitute a violation of section 5741 of the Wiretap Act to access information on an individual cell phone because the cell phone is not a "facility" through which "an electronic communications service is provided." The school officials argued that what the Pennsylvania legislature intended with this provision was to prohibit unlawful access to telecommunications centers and other centralized telephone operations – hence the use of the word "facility."

The court, however, declined to adopt the school officials' position and allowed this claim to proceed. At this early

stage of the litigation, the court believed it best to leave this issue open until the record in the case was more fully developed. In the court's own words: "we decline to make any finding at this time as to the proper limits of the term 'facility.'" The court did, however, find "more persuasive" some of the school officials' arguments regarding the intent of the Pennsylvania legislature in the use of the term "facility," so it is possible that the school officials would ultimately have succeeded in convincing the court that section 5741 of the Wiretap Act does not apply to individual cell phone access. It appears that the court allowed this claim to proceed in part because of the possibility that

Continued on next page

accessing the student's cell phone voicemail – which the plaintiff alleged occurred – may have involved the retrieval of data actually stored by the cell phone service provider.

On some other issues related to this claim, the court ruled in the school officials' favor. The court found that the school officials' conduct in accessing the call log and phone numbers' directory from the plaintiff's cell phone did not violate the Wiretap Act. The court concluded that the call log and phone numbers from the cell phone were not "communications." Comparing the caller identification function on a cell phone to the phone number identification feature of a pager, the court concluded that the Wiretap Act's exclusion of "any communication made through a tone-only paging device" from the definition of "communications" applied to cell phone caller identification information. The court found that the caller identification function on a cell phone merely "records the identity of the caller, but does not allow for the communication of any information," in the same way that a pager simply identifies the number of the person paging. Although the court provides a sound rationale for why cell phone call records do not qualify as "communications" under the Wiretap Act, this situation is yet another instance of the law not keeping up with technological developments. It would strike most people as odd that the closest analogy that the court could find in the statute to a cell phone's call records function is to a "tone-only paging device." It is this writer's opinion that the Pennsylvania legislature should undertake a complete overhaul of the Wiretap Act to bring it into line with current technological developments and with contemporary notions of people's reasonable expectations of privacy in electronic communications.

This brings us back to an earlier statement in this article: school principals face tremendous pressures in making on-the-spot decisions that implicate legal issues, some of which confound lawyers and judges. The problems presented by cell phone technology are particularly difficult.

As cell phone technology becomes more sophisticated, the law governing its access by public officers, including school officials, will need to adapt to these changes. Acting as prudently as circumstances will allow, however, is always the right call.

Here are some basic guidelines school principals should keep in mind when addressing cell phone issues:

- Be familiar with the school district's policy and administrative procedures, including any provisions in a student handbook or a student code of conduct, regarding administrative searches and seizures.
- For search of a student's possessions (other than as part of a general search of all students), there must be a reasonable suspicion based on articulable circumstances that the student is in possession of materials in violation of the law or school district policy.
- Where a student's cell phone is involved in a violation of school policy, be clear as to what aspect of the student's use or possession of the cell phone violates school policy. If activation or operation of the cell phone during school hours is a violation of school policy, then it is lawful to "seize" the phone when a school staff member witnesses a violation of the policy. If there is a reasonable suspicion that the student's cell phone contains evidence of a violation of school policy (for example, a threatening text message), then the phone can be confiscated. In most instances, however, it is advisable not to retrieve the cell phone's text messages, voicemail or other stored information unless the prior consent of the student and the student's parents is obtained.
- Where there is a suspicion that the cell phone contains evidence of illicit activity, such as drug dealing, the more prudent course is to contact the local police authorities, rather than immediately seek to retrieve information from the phone. There is always the risk that in seeking to retrieve evidence from a cell phone, one could inadvertently erase it, which is why it is usually better to leave that type of activity to properly-trained local police officers.

Footnotes:

[1] 425 F.Supp.2d 622 (E.D. Pa. 2006). The facts of the case as described in this article are as they appear in the federal court's decision. Because of the procedural posture of the case, however, the court was required to accept as true all of the allegations in the plaintiff's complaint, many of which the school district denied.

[2] Act 164 of October 4, 1978, P.L. 831, *as amended,* 18 Pa.C.S. § 5701 *et seq.*

[3] 469 U.S. 325 (1985).

[4] *Commonwealth v. Cass,* 709 A.2d 350 (Pa. 1998); *In re FB,* 726 A.2d 361 (Pa. 1999); and *J.S. ex rel. H.S. v. Bethlehem Area School District,* 807 A.2d 847 (Pa. 2002).

[5] 18 Pa.C.S. § 5725.

[6] 18 Pa.C.S. § 5708.

[7] 18 Pa.C.S. § 5725(a).

[8] 18 Pa.C.S. § 5741(a).