National School Boards Association
cosa
Council of School Attorneys

But It's My Cell Phone: Methods and Consequences of Using a Personal Device for School Business

Rachel Hitch
Brandon McPherson
Schwartz & Shaw, Raleigh, NC

Presented at the 2018 School Law Seminar, April 5-7, San Antonio, TX

But It's My Cell Phone:

Methods and Consequences of Using a Personal Device for School Business

Rachel Hitch and Brandon McPherson

Schwartz & Shaw, P.L.L.C.

"Technology is a useful servant but a dangerous master." *Christian Lous Lange*

I. Introduction

Technology has transformed how people communicate with each other. Prior to the proliferation of the telephone, society depended on face-to-face meetings or the written word to communicate with each other. Like society, schools depended on those means of transmitting information. However, by the 1960s society and schools were dependent upon the telephone to communicate important information.

Now fifty years later, our phones have become "smarter" and society, including and maybe especially schools, are saturated with electronic means of communication. Modern societal expectations have evolved such that people demand constant and continuous communication, and school districts have tried to oblige. Most school districts in 2018 are conducting business using mobile phones, electronic mail, automated phone messages, text messaging, school and district websites, education applications, social media, weblogs, video messaging, and video-logs. Technology is beneficial in that it provides parents, students, and school employees with a quick and efficient way to communicate information and conduct business within the school community. Many districts are providing technology devices to some of their employees. However, many times, school business is being conducted on personal devices. Nearly every school employee has access to a personal cell phone, the vast majority of them with "smart" capabilities (e.g., internet access, applications, video capability), and many employees have access to a personal computer, tablet, iPad or Chromebook. In this digital age, school employees often are using a combination of school district devices and their personal devices to communicate within the school community and conduct school business. School personnel's use of their personal devices to conduct school business has several legal implications for school districts, some easily foreseen by school administrators and attorneys, but some less so. The role of the school attorney in this arena is to ensure that potential issues are made known to the district, and to help the district navigate prevention and response efforts.

In the remainder of this paper, we will explore the legal framework surrounding the legal issues that arise when school business, including communication within the school community, is conducted on the personal devices of school personnel. As the legal framework lags significantly behind technological developments, we will discuss the application of that legal framework in an ever-advancing technological society. Finally, we will provide practical pointers for advising clients on avoiding legal battles related to employee use of personal devices to conduct school business.

II. The Legal Framework

Schools have a responsibility to stay current with technology. Just think of the students who were dropped off for kindergarten at the start of the 2017-18 academic year. Schools are tasked with preparing those students to be successful in college and the workforce in 2030 and beyond. Schools attempt to stay current with their methods of communication, but it has not been easy. In the past twenty years, the education system in the United States has seen an accelerated evolution in the frequency and methods by which school districts communicate with parents and students, and the use of technology as a method of delivering instruction. However, the laws and regulations that inform and direct how school districts manage the use of technology by employees have not kept up with the lightning pace of technology development.

A. Search and Seizure issues

For Fourth Amendment purposes, when a school district employee is being investigated, there are two distinct types of investigations: (1) criminal investigations and (2) non-criminal investigations. Criminal investigations of employees are typically led by law enforcement with school personnel playing a secondary role. If there is a search of the employee's personal device, law enforcement will be directing the search of the employee's device. In non-criminal investigations, however, the school district decides whether to search an employee's personal device.

One major concern presented by the use of personal devices to conduct school business is the lack of school district access to information on the device if information on the device is needed. Contexts in which access issues arise include, for example, employee misconduct (e.g., there is evidence on the personal device of employee misconduct), student records (e.g., the need to retain or produce education records), and during litigation (e.g., collecting information that must be produced in discovery or which the school district wishes to use as evidence). In trying to obtain evidence stored on an employee's personal device, school districts and administrators can easily run afoul of search and seizure parameters.

1. Searches by Public Employers

The Fourth Amendment of the United States Constitution protects the "rights of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." [1] The protections made applicable by the 4th Amendment are extended and placed upon state and local governments, including school districts, by the Fourteenth Amendment.[2] "Searches and seizures by government employers or supervisors of the private property of

[1] U.S. Const. Amend. IV.

[2] *New Jersey v. T.L.O.*, 469 U.S. 325, 334-335, 105 S.Ct. 733, 738-739 (1985).

their employees, therefore, are subject to the restraints of the Fourth Amendment."[3]

O'Connor v. Ortega, 480 U.S. 325, 105 S.Ct. 733 (1985).

The seminal case analyzing search and seizure in the context of *public* employment was *O'Connor v. Ortega.* Dr. Ortega was a physician at a state-owned hospital for seventeen (17) years until his dismissal from that position. His primary responsibility was for training young physicians in psychiatric residency programs.[4] Dr. Ortega became the subject of allegations of mistreatment of residents and sexual harassment of female hospital employees.[5] The hospital placed Dr. Ortega on paid administrative leave while the allegations against him were investigated.[6] As part of the investigation, the hospital searched Dr. Ortega's office to secure and inventory the state-owned property located in his office.[7] Typically, searches and inventories of hospital property did not occur until after an employee was terminated. The search of Dr. Ortega's office included desk drawers and filing cabinets.[8] The investigators seized several items from Dr. Ortega's office, including a Valentine's Day card, a photograph, and a book of poetry all sent to Dr. Ortega by a former resident physician.[9] These items were later used to impeach the credibility of the former resident physician when testifying during Ortega's appeal before the State Personnel Board.[10]

Dr. Ortega filed suit against the hospital, alleging among other things violation of his Fourth Amendment rights against unreasonable search and seizure of his office. The District Court granted summary judgment for the hospital, concluding that the search of Dr. Ortega's office was reasonable.[11] The Ninth Circuit Court of Appeals affirmed in part and reversed in part, finding that Dr. Ortega had a reasonable expectation of privacy in his office and that the hospital's search violated the Fourth Amendment.[12]

The case went to the United States Supreme Court. In an opinion delivered by Justice O'Connor, writing on behalf of a plurality of the court, the Supreme Court established a two-part test to be applied in determining whether a 4th Amendment violation has occurred during a non-criminal workplace search. To determine if a violation of the 4th Amendment has occurred Courts should

[3] *O'Connor v. Ortega*, 480 U.S. 709, 715, 107 S.Ct. 1492, 1496 (1987).
[4] *Id.* at 712.
[5] *Id.*
[6] *Id.*
[7] *Id.* at 712-713.
[8] *Id.* at 713.
[9] *Id.*
[10] *Id.*
[11] *Id.* at 714.
[12] *Id*.

decide: 1) whether the employee has a reasonable expectation of privacy in the area being searched (this determination is made on a case-by-case basis), and 2) whether the search was reasonable under the circumstances.

The Supreme Court held that, when determining whether an employee has a reasonable expectation of privacy, the "operational realities of that particular workplace" must be taken into account.[13] The opinion noted that "public employees' expectations of privacy in their offices, desks, and filing cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."[14] One of the factors considered by the Court was that there was "no evidence that the hospital had established any reasonable regulation or policy discouraging employees such as Dr. Ortega from storing personal papers and effects in their desks or filing cabinets."[15] The Supreme Court ultimately concluded that based on all the evidence, including the absence of any policy or regulation by the hospital, Dr. Ortega had a reasonable expectation of privacy in his desk and filing cabinets.[16]

Justice O'Connor then turned to the reasonableness of the search conducted. Harkening back to *New Jersey v. T.L.O.*, 469 U.S. 325, 337, (1985), Justice O'Connor wrote that "what is reasonable depends on the context within which a search takes place."[17] The Court held that in determining the reasonableness of a search, one has to "balance the invasion of the employee's legitimate expectations of privacy against the government's needs for supervision, control and the efficient operation of the workplace."[18] The plurality then considered the needs of the government employer to supervise, control and operate a workplace, including the frequent need to enter the offices and desks of their employees to retrieve state property or records, or to investigate suspected employee misfeasance.[19]

In *O'Connor*, the Supreme Court concluded that "public employer intrusions on the constitutionally protected privacy interests of government employees for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged on the standard of reasonableness under all the circumstances." This reasonableness standard, requires that the search be reasonable at the inception and in the scope of the intrusion.[20]

---

[13] *Id*. at 717.
[14] *Id*. at 718.
[15] *Id*. at 718.
[16] *Id*. at 719.
[17] *Id.* at 718.
[18] *Id.*at 719-720.
[19] *Id*. at 721-722.
[20] *Id*. at 726.

Specifically, "a search of an employee's office by a supervisor will be ***justified at its inception when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a non-investigatory work-related purpose such as to retrieve a needed file***."[Emphasis added][21] Further, "a search will be ***permissible in scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct***."[Emphasis added][22] At this point in the *O'Connor* decision, the plurality determined that while they were able to set a standard, they did not have enough factual evidence to conclude whether the search at issue was reasonable.

Justice Scalia, who concurred in the judgment but disagreed with the rationale, objected to the formulation of what he referred to as a "standard so devoid of content that it produces rather than eliminates uncertainty in the field."[23] Justice Scalia would have held as a general matter that the "offices of government employees, and *a fortiori* the drawers and files in those offices, are covered by the Fourth Amendment protections as a general matter."[24] Justice Scalia stated that he "would hold that the government's search to retrieve work-related materials or to investigate violations of workplace rules – searches of the sort that are regarded as reasonable and normal in private employer contexts, do not violate the Fourth Amendment."[25] However, Justice Scalia agreed that the Court did not have adequate facts and believed that the decision to reverse the Court of Appeals and remand the matter was appropriate.

2. Ownership of the Device: Does it Matter and Why?

City of Ontario v. Quon, 560 U.S. 746, 750, 130 S.Ct. 2619, 2624 (2010).

The 2010 case of *City of Ontario v. Quon*, went beyond *O'Connor* to address to what extent, if any, a public employee has an "expectation of privacy" in personal content on employer-owned technology. There are no Supreme Court cases on a government employer's (non-criminal) search and seizure of an employee's personal device, thus extrapolations from *Quon* have dominated the discussion of what courts might decide with regard to privately owned technology.

[21] *Id*.
[22] *Id*.
[23] *Id*. at 730.
[24] *Id*. at 731.
[25] *Id*.

The City of Ontario, California operates the Ontario Police Department (OPD).[26] Jeff Quon (Quon), was employed by the police department as a Sergeant and a member of the Special Weapons and Tactics (SWAT) team.[27]

In October of 2001, the city purchased twenty (20) alphanumeric pagers capable of sending and receiving text messages.[28] The city's service contract with Arch Wireless allotted to each pager a certain number of characters that could be sent or received each month before incurring an overage fee.[29] The city issued the pagers to the SWAT team, including Quon, to assist in communication and mobilization of the unit.[30] Prior to purchasing and distributing the pagers, the city had adopted a "Computer Usage, Internet and E-mail policy" that applied to all employees.[31] The policy read, in part, that "the city reserves the right to monitor and log all network activity including email and internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources." [32]

Quon signed a statement acknowledging that he had read and understood the computer policy in March 2000.[33] While the computer policy did not address text messages specifically, in April of 2002, through a staff meeting and written memorandum signed by Chief of Police Lloyd Scharf (Chief), police personnel were informed that the city would apply the policy to text messages in the same way it applied to emails.[34]

Within the first two billing cycles, Quon had exceeded his character limit twice.[35] Lieutenant Stephen Duke, Quon's supervisor, and the officer responsible for the city's contract with Arch Wireless, "told Quon about the overages and reminded him that the messages sent to the pagers were considered email and could be audited."[36] Lieutenant Duke went on to tell Quon that "it was not his intent to audit an employees' text messages to determine if the overage was due to work-related transmission" and recommended that Quon reimburse the city for the overage fee instead of having his text messages audited.[37] Quon then wrote a check for the amount.[38]

---

[26] *City of Ontario, Cal v. Quon*, 560 U.S. 746, 750, 130 S.Ct. 2619, 2624 (2010).
[27] *Id*.
[28] *Id*.
[29] *Id*. at 750-751.
[30] *Id*. at 751.
[31] *Id*.
[32] *Id.*
[33] *Id.*
[34] *Id*. at 751-752.
[35] *Id*. at 752.
[36] *Id.*
[37] *Id*.
[38] *Id.*

Within the next few months, Quon repeatedly exceeded his character limit. This prompted the Chief to direct Lieutenant Duke to determine "whether the existing character limit was too low" (meaning that the officers using the phone for work-related purposes did not have enough characters and were being forced to reimburse for work-related expenses) or, instead, "if the overages were because of personal matters."[39]

The Chief directed Lieutenant Duke to request transcripts of text messages sent in August and September by Quon and the other employees who had exceeded the character allowance.[40] Duke requested this information from the wireless carrier, reviewed the transcripts and discovered that many of the messages sent and received on Quon's pager were not work-related and some were sexually explicit.[41]

The Chief shared this information with Internal Affairs which began an investigation.[42] The investigation discovered that Quon had sent or received 456 messages during work hours in the month of August 2002, of which no more than 57 were work-related. Quon had sent as many as 80 text messages during a single day at work.[43]At the conclusion of the Internal Affairs investigation, Sergeant Quon was allegedly disciplined.[44]

Quon filed suit in the United States District Court for the Central District of California, raising claims under Section 1983, the Stored Communications Act, and California law.[45] The Stored Communications Act established criminal and civil consequences for electronic communication service providers if they release information about their customers communications without legal consent or as otherwise authorized by law.[46] In addition to Quon, other plaintiffs included individuals whom Quon had exchanged text messages with during August and September 2002, including Jerilyn Quon, Quon's then wife from whom he was separated, April Florio, a police department employee with whom Quon was romantically involved, and another member of the SWAT team.[47]

The parties filed cross-motions for summary judgment. The District Court granted Arch Wireless' motion for summary judgment on the Stored Communications Act claim, but denied all defendants' motions for summary

[39] *Id.*
[40] *Id.*
[41] *Id*. at 753.
[42] *Id*.
[43] *Id*.
[44] *Id*.
[45] *Id.*
[46] 18 U.S.C. §§ 2701-2712. The Stored Communications Act is addressed in more detail below in Section 6.
[47] *Quon* at 753.

judgment on the Fourth Amendment claim.[48] Based on the plurality opinion in *O'Connor v. Ortega*, the District Court decided that Quon had a reasonable expectation of privacy in the content of his text messages.[49] The remaining issue was whether the audit of Quon's text messages was nevertheless reasonable.[50] The District Court decided that this turned on a question of the Chief's intent.[51] The District Court held a jury trial to determine the purpose of the audit, and the jury concluded that the Chief ordered the audit to determine the sufficiency of the character limits.[52] As such, the Court held that the defendants did not violate Quon's Fourth Amendment rights.

The case was appealed to the Ninth Circuit Court of Appeals where the lower court was reversed, in part. The panel agreed that Quon had a reasonable expectation of privacy in his text messages but found the search unjustified.[53] The Court of Appeals also concluded that Arch Wireless had violated the Stored Communications Act by turning over the transcript to the city.[54]

The Supreme Court granted the petition for certiorari filed by the city, the police department and Chief Scharf. At the outset the Court warned against applying a broad standard concerning employees' privacy expectations vis-a-vis employer provided technological equipment, as "[r]apid changes in the dynamics of communication and information transmission are evident not just in technology itself but in what society accepts as proper behavior."[55] The Court went on to state:

> Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one can counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent such policies are clearly communicated.[56]

---

[48] *Id.* at 754.
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.* at 755.
[55] *Id.* at 759.
[56] *Id.* at 760.

The Court then made three important points for purposes of its decision in *Quon*:

1. Quon had a reasonable expectation of privacy in this text message on the pager provided to him by the city;
2. The city's review of the transcript constituted a search within the meaning of the Fourth Amendment; and
3. The principles applicable to a government employer's search of an employee's physical office apply with at least the same force when the employer intrudes on the employee's privacy in the electronic sphere.[57]

The Court then applied the *O'Connor* plurality approach and held that:

> "when conducted for a non-investigatory, work-related purpose or for the investigation of work-related misconduct, the government employer's warrantless search is reasonable ***if it is justified at its inception and if the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the circumstances giving rise to the search***." [Emphasis added][58]

Based on that standard, the Court decided that the search was reasonable.

The Court first looked at whether the search was justified at its inception and used the jury's determination that the city's purpose for the search was to determine whether the character limit on the city's contract with Arch Wireless was sufficient to meet the city's needs.[59]

Next, the Court reviewed the scope of the search and determined that it was reasonable, disagreeing with the Court of Appeals.[60] Specifically, the Court reasoned that the limits placed on the search, i.e., looking only at the August and September transcripts to obtain a large enough sample to decide whether the character limit was sufficient, was reasonable.[61] Further, for the Internal Affairs investigation, the department redacted all messages Quon sent while off duty to reduce the intrusiveness of any further review of the transcripts.[62]

The Court explained that the appellate court's holding would have required the least intrusive search practicable. The Court reasoned that this did not

---

[57] *Id.*

[58] *Id.* at 761.

[59] *Id.*

[60] *Id.* at 765.

[61] *Id.* at 761.

[62] *Id.* at 762.

comply with precedent or the practical realities of being a government employer.[63]

The Court was not convinced by Quon's argument that the search was unreasonable because Arch Wireless violated the Stored Communications Act in turning the transcripts over to the City of Ontario.[64] While that issue was not before the Court, Quon was unable to point to any authority "for the proposition that the existence of a statutory protection renders a search *per se* unreasonable under the Fourth Amendment."[65] There was also no allegation that the City of Ontario realized it was violating the law or should have known it was violating the law when it requested the transcript be turned over to them.[66]

The Court then held that the search was motivated by a legitimate work-related purpose and was not excessive in scope and thus was reasonable under the *O'Connor* plurality.[67]

The Court majority opinion mentioned but did not decide whether the search violated the Fourth Amendment rights of the other individuals who were communicating with Quon via text message on his employer provided pager.

3. Does the Format/Device Matter?

Quon has been applied in several cases involving different forms of technology:

A. Cell Phones

Larios v. Lunardi, 2016 WL 6679874 (E.D. Cal. Nov. 14, 2016).

Some lower courts have begun to tackle the issue of a government employer's search of an employee's personal cell phone. *Larios v. Lunardi* applies the principles of *Quon* to a government employer's search of an employee's personal cell phone. Plaintiff Larios was a member of the California Highway Patrol (CHP). Larios had been issued a CHP cell phone but also maintained a personal cell phone. When Larios became the subject of an internal CHP investigation for alleged misconduct, he turned over to CHP his CHP-issued phone. Larios was later told that he had to turn over his personal phone to "conduct a data extraction to retrieve all work product."[68] Under

[63] *Id.* at 763-764.
[64] *Id.* at 763.
[65] *Id.* at 764.
[66] *Id.*
[67] *Id.*
[68] *Id*. at *1.

threat of "charges/disciplinary action," Larios turned over his personal phone. When Larios' phone was returned to him, phone calls had been made from it and "all of the information stored on the phone had been searched and downloaded."[69] Larios filed suit.

The District Court rejected the defendants' claim that a CHP policy justified the search of Larios' personal cell phone. Where the policy provided that "[w]ork stored on any type of electronic device is the property of the state and must be relinquished upon demand." However, the District Court held that the policy was "silent" as to whether CHP officers had to submit their personal cell phones to such inspection.[70]

The court relied heavily on the fact that the plaintiff's personal cell phone had personal information as well as "work product" and everything else on that same phone. Larios had, with the permission of his employer, used his personal cell phone to conduct CHP work, but: "Knowing that work product would remain open to inspection in no way puts an employee on notice that the government will also have carte blanche to review everything an employee keeps on his or her phone."[71] The court analogized this to an employee (with permission) keeping work files at his house. Having files at one's house, reasoned the District Court, does not open up the rest of the house to search simply because those files are there.[72] On this point, the court invoked the rationale from the Supreme Court's decision in *Riley v. California* that "[a] phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone [itself] is."(quoting *Riley v. California*, 134 S. Ct. 2473, 2491 (2015)). Thus, the District Court held that "the measures purportedly adopted by Defendants to search Plaintiff's phone were not at all reasonably related to the objectives of the search and were, to the contrary, excessively intrusive under the circumstances."[73]

B. Electronic Mail

Hoofnagle v. Smyth-Wythe Airport Commission, 2016 WL 3014702 (W.D. Va. May 24, 2016).

[69] *Id*. at *2.
[70] *Id*.
[71] *Id.* at *4.
[72] *Id.*
[73] *Id.*

Another case to apply the *Quon* analysis was *Hoofnagle v. Smyth-Wythe Airport Commission*.

In *Hoofnagle*, the court considered whether the Smyth-Wythe Airport Commission (Commission) violated the Fourth Amendment rights of Charles H. Hoofnagle by reviewing a Yahoo email account which Hoofnagle used for both personal and business purposes.[74] Also worth noting here is that the Commission was a public entity and a political subdivision of counties and towns. Mr. Hoofnagle was the Operations Manager of Mountain Empire Airport and his job was to maintain the day-to-day operations of the airport.[75]

After the Newtown, CT mass school shooting, United States Senator Tim Kaine sent a letter to Hoofnagle addressing the issue of gun violence, which was apparently a response to an earlier communication on the issue from Hoofnagle to Senator Kaine.[76]

By an email sent February 16, 2013, Mr. Hoofnagle blasts and berates Senator Kaine for his position on gun issues. Mr. Hoofnagle signs this email "Airport Operations Manager, Mt. Empire Airport."[77] Shortly after seeing this email, the Commission terminated Mr. Hoofnagle's employment. The chair of the Commission then accessed Mr. Hoofnagle's Yahoo email account, using the password provided by the airport secretary in order to retrieve business records of the airport.[78] There is disagreement regarding whether Mr. Hoofnagle authorized the Commission or its members to access his email account.

The court used the *Quon* court's analysis to come to the conclusion that Mr. Hoofnagle's Fourth Amendment rights were not violated.[79] The court established at the outset that Mr. Hoofnagle had a reasonable expectation of privacy in his email account and the only question that remained was the reasonableness of the search. The court reasoned that the Commission's search of Mr. Hoofnagle's email for business records was reasonable at its inception and was reasonable in scope because the Chair of the Commission only viewed Mr. Hoofnagle's account for 30-40 minutes to determine whether

[74] *Hoofnagle* at *1.
[75] *Id.*
[76] *Id.*
[77] *Id.* at *2.
[78] *Id.*
[79] *Id.* at *9.

there were any emails that contained important airport business that they needed to preserve.[80]

4. Practical Advice for Workplace Investigations

The most significant context for employment issues arising from employee use of personal technology are workplace investigations.

As stated previously, the most common type of investigation is the non-criminal investigation of employees who have engaged in misconduct, and evidence of the misconduct is captured on the employee's personal device. The issue then becomes whether the school district can search the employee's personal device. This is when your knowledge as a school attorney is essential.

School districts are government employers and are limited by the Fourth Amendment. Therefore, *Quon* and *O'Connor* are instructive on how to address this issue. First, we must determine whether an employee has a reasonable expectation of privacy in his or her personal device. This is a case-by-case determination, but given the treatment by earlier courts, we believe that the accused school employee will likely have a reasonable expectation of privacy in his or her personal device.[81] The employee's expectation of privacy can be limited by a board policy. For example, a board policy that informs the employee that school business records, wherever found, including personal devices, are subject to search by school personnel, could limit the employee's expectation of privacy.

The second question is whether the school district's search is reasonable, both at its inception and in the scope of the search. A search is "***justified at its inception when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a non-investigatory work-related purpose such as to retrieve a needed file***." [Emphasis added][82] "A search will be permissible in scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct."[83] Based on *Larios v. Lunardi*, a search of an employee's entire personal phone for work product would likely not be considered reasonable.[84] At this point in the analysis, the school district must determine the reason and scope of the search of the employee's personal device.

---

[80] *Id.*

[81] *City of Ontario v. Quon*, 560 U.S. 746, 759 (2010).

[82] *O'Connor v. Ortega*, 480 U.S. at 726.

[83] *Id*.

[84] 2016 WL 6679874 at *4.

Also, to be considered are the consequences the school district faces for not gaining access to the information contained on the employee's personal device. Is the information school business? Is the information contained on the personal device a public record? Is the employee the only person who is in possession of the information? What is the potential for litigation with this employee as a result of the search?

5. State Constitutional Provisions

In addition to the Fourth amendment protections provided above, board attorneys need to consider the applicability and case law of their particular jurisdiction when considering state constitutional protections against unreasonable searches and seizures. Specifically, ten state constitutions have explicit clauses addressing or related to right of privacy. Most of these state constitution privacy protections mirror the Fourth amendment, while some have significant differences. For example, Article I, Section 4 of the Florida Constitution provides "the right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated."

Particularly relevant to our topic is a recent amendment to the Missouri state constitution. In August 2014, the people of Missouri voted to approve Amendment IX to the state constitution which revised Article I, Section 15. Amendment IX provides constitutional protections from unreasonable searches and seizures for electronic data or communication such as that found on cell phones and other electronic devices. While expectations of privacy are subject to change, interpretations of state constitutions that provide protection for electronic communications will likely be slow to change, but should be monitored regularly.

6. Stored Communications Act

In addition to Fourth Amendment and State provisions relating to employee privacy, in 1986 Congress adopted the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712, which limits the public school district's ability to obtain information stored on a personal cell phone from a third-party provider. The SCA was created in response to the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735, 99 S. Ct. 2577 (1979). In *Smith*, the Court held that a criminal defendant's Fourth Amendment rights were not violated by the installation of a pen register by the telephone company at the request of law enforcement.[85] The Court reasoned that the defendant did not have a

[85] *Smith* at 745-746.

reasonable expectation of privacy in numerical information he voluntarily conveyed to the telephone company.[86]

The SCA creates criminal and civil consequences for a third-party electronic communication service provider (ESP) if it releases electronic communications, like emails and text messages, to government actors or private parties without an applicable exception.[87] For instance, Verizon Wireless is an ESP that provides electronic communications and storage for its customers. The SCA prevents Verizon Wireless from releasing the records of its customers' communications or the contents of those communications except as permitted by the statute.

Voluntary Disclosure

An ESP can release a log of communications (not including the contents of communications)[88] in the following circumstances:

1. When compelled disclosure to law enforcement is required by 18 U.S.C. § 2703;[89]
2. "With the lawful consent of the customer or subscriber;"[90]
3. When the release is necessary to provide the service or to protect the rights or property of the ESP;[91]
4. When the release is "to a governmental entity, if the [ESP], in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;"[92]
5. When the release is to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;[93] or
6. "to any person other than a governmental entity."[94]

[86] *Smith* at 743-744.
[87] 18 U.S.C. §§ 2701-2712.
[88] 18 U.S.C. § 2702(c).
[89] 18 U.S.C. § 2702(c)(1).
[90] 18 U.S.C. § 2702(c)(2).
[91] 18 U.S.C. § 2702(c)(3).
[92] 18 U.S.C. § 2702(c)(4).
[93] 18 U.S.C. § 2702(c)(5).
[94] 18 U.S.C. § 2702(c)(6). This exception is broad. However, the legal reasoning behind this exception is that the log of communication is the property of the ESP and it should be able to share its property with whomever it wishes except governmental entities.

An ESP can "divulge the contents of a communication"[95] if at least one of the following apply:

1. The release is to an addressee or intended recipient or their agent;[96]
2. The release is otherwise authorized by law or court order pursuant to 18 U.S.C. § 2517 (permits wiretapping or call interception by law enforcement), 18 U.S.C. § 2511(2)(a) (permits limited wiretapping or call inception by service providers to protect the rights or property of the provider), or 18 U.S.C. § 2703 (addresses compelled disclosure of the contents of communications maintained by ESPs);[97]
3. The release is "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;"[98]
4. The release of the communication is "to a person employed or authorized or whose facilities are used to forward such communication to its destination;"[99]
5. The release is necessary to provide the service or to protect the rights or property of the ESP;[100]
6. The release is to the National Center for Missing and Exploited Children, in connection with a report submitted pursuant to 18 U.S.C. § 2258A;[101]
7. The release is to a law enforcement agency when (i) the contents were inadvertently obtained by the ESP; and (ii) appear to pertain to the commission of a crime;[102] or
8. The release is "to a governmental entity, and the [ESP], in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[103]

These strict limitations on ESPs make it nearly impossible for a school district to obtain access to the content of electronic communications without the consent of the customer, an addressee or an intended recipient.

---

[95] 18 U.S.C. § 2702(b).
[96] 18 U.S.C. § 2702(b)(1).
[97] 18 U.S.C. § 2702(b)(2).
[98] 18 U.S.C. § 2702(b)(3).
[99] 18 U.S.C. § 2702(b)(4).
[100] 18 U.S.C. § 2702(b)(5).
[101] 18 U.S.C. § 2702(b)(6).
[102] 18 U.S.C. § 2702(b)(7).
[103] 18 U.S.C. § 2702(b)(8).

Compelled Disclosure

An ESP can be compelled to disclose the contents of communications or records of communications only when:

1. The ESP is issued a search warrant pursuant to Federal or State Rules of Criminal Procedure (no notice to the customer is required);[104]
2. Prior notice is given to the customer by the governmental entity, and the ESP is issued an administrative subpoena pursuant to a Federal or State statute, a grand jury, or a trial subpoena;[105] or
3. Prior notice is given to the customer by the governmental entity, and the ESP is presented with a court order pursuant to 18 U.S.C. § 2703(b).[106]

The SCA provides no exception that permits an ESP to release the contents of electronic communications pursuant to a civil subpoena. This issue has been argued multiple times with the same outcome.[107]

III. Miscellaneous Issues Presented by School Business Conducted Via Personal Technology

The issues presented by school business being conducted via personal technology are many and as varied as the school districts having to resolve them. Below are a few of the key issues that seem to commonly arise.

A. School District Statutory and Regulatory Compliance Issues

1. Public Records/Sunshine Laws

Always present in any discussion of electronic records relating to schools is public records laws. In the post-Watergate era all states have passed public record or sunshine laws to provide for a transparent government. These laws uniformly apply to political subdivisions including school boards. Most state laws provide for a comprehensive definition for what constitutes a public record. In the digital age, the definition of public record has expanded as technology has advanced. With the advent of electronic mail, iPads, iPhones

[104] 18 U.S.C. § 2703(a) and (b).

[105] 18 U.S.C. § 2703(b).

[106] 18 U.S.C. § 2703(b).

[107] *In re Subpoena Duces Tecum to AOL*, LLC, 550 F.Supp.2d 606 (E.D.Va.2008); *J.T. Shannon Lumber Company, Inc. v. Gilco Lumber Inc.*, 2008 WL 4755370 (N.D. Miss. 2008); *Mintz v. Mark Bartelstein & Associates, Inc.*, 885 F. Supp. 2d 987, 991 (C.D. Cal. 2012).

and other devices, the types and amounts of information that fit the definition of a public record has grown exponentially.

Most state public records laws provide that public records, regardless of format or location, remain public records subject to public inspection. Cases have developed regarding email, text messages and electronically stored data that would be a public record if in print within the school district. Courts have found that those "records" maintain their public nature (unless protected from public disclosure by some exemption to the public records statute). For school boards that deal with various sensitive confidential information regularly, public records often contain both public information and confidential student information.

Recently, two state supreme courts ruled that the content of personal cell phones, including text messages, are public records if sent by officials in their official capacity. Despite the fact that the communications at issue both in *Nissen v. Pierce County*, 183 Wash.2d 863 (2015) and *City of San Jose v. Superior Court,* 2 Cal.5th 608 (2017), were sent over and stored on a private cell phone, the analysis returned to determining whether the content of the record makes it a public record.

Just like its paper counterpart, whether an electronic record is a public record is determined by its author, content, and storage. The basic question to ask in determining whether an electronic record is a public record is, "Was it created in the furtherance of public business?" The electronic communication and innovation of the digital age leads us to depend more on technology to assist in ensuring compliance with public records laws. While data may be housed in more than one location, including on personal cell phones, school districts find themselves playing catch up to ensure their policies and procedures protect students and staff alike.

2. Records Retention Issues

Many educators are unaware that the records they have on their personal devices may be subject to a state records retention schedule. When the school district is unaware that the record exists, or is unable to obtain the record from the employee's personal device, they may run afoul of obligations under the applicable records retention requirements.

B. Student Issues

School districts provide student records pursuant to a multitude of authorities requiring such a production. By way of example, but not limitation, parents are entitled to access student records, state agencies may be entitled to review student records, and OCR or other federal agencies may be entitled to student records. One of the primary challenges for school districts when responding to

these requests is identification and collection of all the responsive records. In the context of this article, does the school district know that a record exists on an employee's personal device that is responsive to the request? School employees sometimes send emails or text messages or keep other information on their personal devices that may be considered responsive, yet the employee is the only person in the school district who knows the record has been created. If no one else has seen the record it might be exempt from some productions (e.g., under FERPA) but the school system is denied the ability to utilize a record that may be helpful to the school system in serving the child or defending against a complaint.

The consequences of a school district not knowing about a record and, being unable to access the record are fairly obvious. If the school district cannot access the record, it cannot release it. To make matters worse, if the requesting party knows the record exists (e.g., the parent was a party to an email) and the school district does not provide the record in its response, the school district could be accused of intentionally withholding information. The good news is that FERPA does not provide a private right of action for parents for alleged violations. The bad news is that under the IDEA the failure to provide records could lead to a due process proceeding. Even worse news is that OCR could broaden an investigation based on a school district's failure to provide information.

1. FERPA

Next, we examine the legal framework regarding electronic communications and the Family Educational Rights and Privacy Act (FERPA).[108]

School personnel often and frequently deal with electronic records that are protected by FERPA. 34 C.F.R. Section 99.3 defines "education records" as "records that are 1) directly related to a student; and 2) maintained by the educational agency or institution or by a party acting for the agency or the institution."[109] The regulation goes on to identify specific exclusions from the definition of "education record," including one that is particularly applicable to electronic communications:

- records that are kept in the sole possession of the maker and are used only as a personal memory aid and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.[110]

When FERPA was enacted, the drafters clearly envisioned a physical file where education records were maintained. However, the modern and digitized

[108] 20 U.S.C. § 1232g.

[109] 34 C.F.R. § 99.3.

[110] 34 C.F.R. § 99.3 b(1).

education system rarely has all education records maintained in a single file (or even in hard copy anywhere). Parents' attorneys and school attorneys often debate whether a document, electronic or otherwise, constitutes an "education record." The dispute frequently hinges on whether the record is "maintained" by the school district as required by 20 U.S.C. § 1232g(a)(4)(A)(ii).

In *Owasso Indep. School Dist. 1-011 v. Falvo*, the United States Supreme Court addressed what is meant by "maintained" for purposes of FERPA. The issue in *Owasso* was whether the practice of allowing students to grade one another's work and call out their own grades violated FERPA. The Court held that a student assignment that is peer-graded does not satisfy the FERPA definition of "education record."[111] The Court's reasoning was, in part, based on its interpretation of when a record is "maintained." The Court said, "the ordinary meaning of the word "maintained" is "to keep in existence or continuance; preserve; retain."[112] The word "maintained" suggested FERPA records would be kept in a filing cabinet in a records room (or central repository) at the school or a permanent secured database, perhaps even after the student is no longer enrolled.[113]

The Court also provided direction in *Owasso* regarding what is meant by "a person acting for an educational institution for purposes of § 1232g(a)(4)(A)."[114] "The phrase 'acting for' connotes agents of the school, such as teachers, administrators, and other school employees."[115]

In applying *Owasso*, a number of courts have used the limited definition of "maintained" to exclude emails from the definition of education records if those emails are not stored in the student's file that is maintained by the district.[116] However, the United States Department of Education's Family Policy Compliance Office ("FPCO") has cast a broader net in determining whether an email constitutes an education record when it is not stored in the student's file. For example, in our personal experience, FPCO has applied FERPA to include as an "education record" an email to a parent explaining why a student received a disciplinary consequence although the email was not kept in the student's file. FPCO made this determination on the basis that the email was directly related to the student and "maintained" by the district on its email server. FPCO's analysis arguably eviscerates the Supreme Court's limited definition of "maintained," or at least for electronic records. School attorneys

---

[111] *Owasso Indep. Sch. Dist. No. I-011 v. Falvo*, 534 U.S. 426, 122 S. Ct. 934, 151 L. Ed. 2d 896 (2002).

[112] *Owasso* at 433.

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] *S.A. ex rel. L.A. v. Tulare County Office of Educ.*, 2009 WL 3126322 (E.D. Cal. 2009); *B.F. v. Fulton County School Dist.*, 2008 WL 4224802 (N.D. Ga. 2008).

facing this issue should carefully monitor case law developments of this issue, particularly in their respective jurisdictions.

2. IDEA

The Individuals with Disabilities Education Act ("IDEA"), 20 U.S.C. 1400 and 34 C.F.R. §300, outlines the rights and responsibilities of school districts regarding education records for students with disabilities. The IDEA incorporates FERPA's definition of "education record."[117] This shared definition of "education records" provides consistency when applying records provisions to students with and without disabilities. 34 C.F.R. § 300.613, Access to Records, directs school districts to permit parents to inspect and review any education records related to their students that are "collected, maintained, or used by the agency."[118] This language mirrors the language in FERPA.

One of the ways in which the IDEA expands upon FERPA is in its timeline for providing records. Under the IDEA, the agency must comply with the request without unnecessary delay and before any meeting regarding a student's IEP, or any hearing pursuant to § 300.507 or §§ 300.530-300.532, or any resolution session pursuant to § 300.510, and in no case more than forty-five (45) days after the parent's request to inspect and review the records has been made.[119]

This IDEA regulation also expands FERPA's requirements with regard to the right to inspect and review education records. The IDEA regulation grants parents "the right to a response from the participating agency to reasonable requests for explanations and interpretations of the records," "the right to request that the agency provide copies of the records containing the information if failure to provide those copies would effectively prevent the parent from exercising the right to inspect and review the records," and "the right to have a representative of the parent inspect and review the records."[120]

These heightened rights, coupled with the lack of clarity as to what constitutes an "education record" that is "maintained" by the school district as it relates to electronic records, leads to conflict in an already adversarial relationship between school districts and parents. In the climate of distrust that often accompanies special education disputes, the failure to provide records that the school district did not believe to be "education records" "maintained" by the agency is often recast as a purposeful and/or deceitful withholding of information. Once in a due process situation, if discovery is allowed in the jurisdiction, when records are provided through discovery that were not provided pursuant to a previous education records request, the due process

[117] 34 C.F.R. § 300.611.

[118] 34 C.F.R. § 300.613(a).

[119] § 300.613(a).

[120] 34 C.F.R. § 300.613(b).

case can quickly be diverted to an allegation of misconduct on the part of school officials with regard to records.

The IDEA differs from FERPA in that, under the IDEA, parents have the right to meaningful participation in their child's individualized educational program (IEP).[121] As part of this participation, parents are entitled to review records in advance of an IEP meeting (as well as some other meetings associated with due process actions). The failure to provide access to education records often ends up playing a role in claims that a student was denied a free appropriate public education (FAPE) where the parent was denied access to records before an IEP meeting (and therefore, as the argument goes, was denied meaningful participation). While parents have access to the same records under IDEA as they do under FERPA, the differing timeline (prior to an IEP meeting under IDEA, versus within a reasonable period of no more than 45 days under FERPA) and the due process implications under IDEA increase the importance of identifying all education records. Put another way, while there is no individual right of action under *Owasso*, IDEA provides a mechanism where the failure to provide access to educational records supports a claim of a denial of FAPE, giving the education records access requirements teeth under IDEA that do not exist under FERPA.

Given that some students with disabilities have an increased number of service providers, and given that communication between staff and parents of students with disabilities is often at a higher frequency than communication between staff members and parents of students without disabilities, the number of records that are potential "education records" under IDEA can be staggering. Access issues with records stored on personal devices can be exacerbated in special education cases. These responses are both costly and cumbersome for school districts. However, FERPA permits school districts to charge a copying fee.[122]

C. Litigation Issues

Finally, the use of personal devices to conduct school district business raises significant litigation issues. Two major issues are e-discovery by opposing parties of the employee's personal device and third-party subpoenas of school business records on the employee's device. E-discovery subjects the employee's personal device, including any electronically stored information, to be inspected, copied, tested, or sampled by the opposing party.[123] Under the Federal Rules of Civil Procedure, if a party wants to object to an e-discovery request, the objection "must state whether any responsive materials are being

[121] 20 U.S.C. § 1415.

[122] 34 C.F.R. § 99.11.

[123] Fed. R. Civ. P. 34.

withheld on the basis of that objection."[124] Further, the "objection to part of a request must specify the part and permit inspection of the rest."[125] This process can be time consuming and expensive for school districts. The school district could also face sanctions from the court for failure to comply with e-discovery.

Equally as unpleasant is a third-party subpoena of the school records contained on the employee's personal device. Those records would have to be turned over to the third-party requester unless and until the subpoena is quashed or the employee is otherwise released from the subpoena. Once again, objecting to the subpoena could be expensive for a school district.

IV. Ten Tips for School Attorneys

As school attorneys, we often see examples of what school personnel should not do when using their personal devices to conduct school business. Here are ten (10) tips for school attorneys when addressing employee use of personal devices.

1. Create a Board policy that clearly establishes the school district's expectations regarding employee use of personal devices for school business

Boards have options for how they deal with employees who use their personal devices for school business. Those options include:

- **Prohibit employee use of personal devices for school business.** This establishes a bright line rule, significantly minimizes the issues outlined above, and provides a very clear expectation for employees (and for any subsequent employee discipline). However, this may significantly inhibit beneficial communication, will likely be unpopular with teachers and parents, and may not prevent use.
- **Permit employees to use their personal devices, but require them to consent to reasonable searches of their devices.** This option would give the employee a choice between (a) not using their personal devices for school business, or (b) using their personal devices for school business, but providing written consent to future searches of their personal devices for school business records. This places the decision at the employee's feet and also clearly addresses what their expectation of privacy is in their personal device. We recommend having the employee make their choice in writing, and affirmatively consent to the search of their device by signing the document. It is also necessary to address in the policy how the employee may revoke their consent and the effect of that revocation.

[124] Fed. R. Civ. P. 34 (c).

[125] Fed. R. Civ. P. 34 (c).

- **Permit employees to use their personal devices, but limit their use to a single application or select group of applications.** This option permits school districts to allow employees to use their personal devices to conduct school business, but only using the media the school district dictates. The district can choose applications that give school administrators access to all communications and content.

This is not an exhaustive list of options. School attorneys should speak with their client and find an option that works best for that client.

2. Address the use of personal devices by employees in collective bargaining agreements (CBA)

As NFL Commissioner Roger Goodell will attest, specifying your power to investigate in the CBA is key.[126] If the issue of personal device use for school business is addressed in the CBA, it can prevent litigation later about the school district's search of employees' personal devices.

3. Provide professional development about the downsides of employee use of their personal devices for school business

If school employees understand the negative aspects of using their personal devices for school business, they will likely choose not to use it. It may help to highlight some of the negative aspects that most directly impact the employee: (a) The employee is opening their personal life to potential review by a court; (b) The employee is giving an increased level of access to themselves for students and parents, which may change expectations regarding communications, and can be burdensome and time consuming; (c) Using a personal device creates the opportunity for the employee's intentions and integrity to be challenged; and (d) The employee is paying for the personal device, not the school district, so they are unnecessarily spending money out-of-pocket for work-related business. Explaining the reasons outlined above could convince employees not to use their personal devices for school business.

4. Address use of personal devices in third-party service provider contracts

Third-party service providers are in frequent communication with school personnel and parents for the students they serve. These providers often create and maintain business records for the district, and often use their personal devices to do so. Sometimes ours control over these service providers is less direct and, with little or no notice, they leave the contract company. Addressing what means are acceptable for those records is important and should be spelled out in the service provider's contract, so that the district has something upon which to take action if the provider stops serving the child or the district and retains important records.

---

[126] *National Football League Management Council v. National Football League Players Ass'n*, 820 F.3d 527, 206 L.R.R.M.(BNA) 3102 (2016).

5. ***When employees leave the district, make sure that any school business records, including those on their personal device, are transferred to the school district***

Likewise, school attorneys should train human resource directors and school administrators to ask employees who are leaving the district to provide all school business records in their possession, including those on the departing employee's personal devices. Addressing this issue while the person is still your employee is far easier than having to address the issue months or years later as part of an OCR complaint or lawsuit.

6. ***Teach school administrators and teachers how to diplomatically refuse to share their personal account information with parents***

Oftentimes having a teacher's personal cell phone number gives parents a sense of security. However, if teachers explain the burdens and issues created by sharing his or her cell phone number, parents are less likely to be upset about the teacher's decision to not share their number. For example, the time spent replying to twenty-eight different text messages or phone calls from parents in the mornings could be better spent preparing for the instructional day. Similarly, parents may understand limitations on the use of employee personal devices if they understand the records issues created by using the employee's personal cell phone, the burdensome nature of extending the locations to search for potential student records, and the end result possibly being that student records are not retrievable for the school district when a parent requests.

7. ***Review any state laws that regulate or prohibit school employee communications with students via electronic communication***

School attorneys need to review state laws regarding school employee communications with students. For example, the Louisiana State Legislature passed a law in 2009 requiring school employees to document any electronic communication within twenty-four hours of creation.[127]

8. ***Thoroughly understand the record retention laws for your jurisdiction***

A school attorney's knowledge of his or her jurisdiction's records retention laws can save your clients time and money. Additionally, it will enable you to know which records must be maintained and which can be discarded.

9. ***Have at least a basic understanding of how different personal devices and applications work***

When advising your clients about regulating electronic devices, it is important to understand the devices themselves. For example, understanding that some personal devices require passcodes or fingerprints to open them, while some newer devices have facial recognition software. Equally as important is understanding how the

[127] La R.S. 17:81(Q).

applications on those devices work in the most basic terms. For example, how do you open the application and what passwords are required to enter the application. This information is necessary to assist the district with understanding the protection of student records housed in each type of device or application.

10. Get to know a forensic computer engineer

Forensic computer engineers and/or service providers are extremely helpful for reviewing cell phones, iPads, tablets and other devices. These professionals can find and discover information not easily found on devices. Additionally, they can help customize e-discovery or recover deleted information.

Plus, an extra tip: If the school attorney is involved in responding to a records request, provide clear written instructions to the client that records on personal devices are included and must be produced, if responsive. If it is ultimately found that someone did not turn over several records, it is better that such failure occurs notwithstanding your instructions, not because of them.

V. Conclusion

As technology advances and the law lags behind, school districts struggle to address the multitude of issues that arise when school personnel use their personal devices for school business. Knowing the issues likely to arise provides an opportunity for the school attorney to advise of preemptive ways of avoiding liability on behalf of school clients.