Towards an Operational Model of On-line Password Ownership for Older Minors

Mark Darius Juszczak

CONTACT: Mark Darius Juszczak, PhD, Department of Mass Communication, St. John’s University, New York, USA, E-mail: mark.darius.juszczak@googlemail.com

Abstract:
This paper is an exploratory study of the current debate, confined primarily to US Supreme Court cases, over the definition of both a password and an older minor, with the intention of highlighting current inconsistencies in definition and classification of the two terms and suggesting how an operational model of on-line password ownership for older minors might develop. Section 1302 of COPPA (Children's On-line Privacy Protection Act) legally defines a child as an individual under the age of 13, and the United States defines 18 to be the legal age at which an individual becomes an adult and enjoys all of the full rights of on-line password ownership & control that may be protected under the First, Fourth and Fifth Amendments to the US Constitution.

Between the ages of 13 and 18, however, there is no clear model or legal guideline with regards to the question of online password ownership – and the extent to which Constitutional Amendment protections are fully enjoined by such individuals. The intention of this paper is to explore the current debate through the lens of US Supreme Court Cases – as such cases both set national precedents for legal action and rights and provide unique insight into the broader social discussion about the critical issue of online password ownership for older minors. The paper will attempt to answer two basic questions: what is the legal nature of a password and what is the legal nature of an older minor? Finally, it will attempt to address the question of how an operational model of online password ownership for older minors in institutional educational settings may evolve.

Keywords:
older minors, online password ownership, the constitutional rights, the legal nature of a password

Introduction

A Cellphone is not just a cellphone anymore. As cellphones become smartphones, they also become digital archives of our real lives. Access to a cellphone today can be more intrusive than any warranted search of a room or locker, or than any interrogation. While privacy and protection of this digital mirror of our lives is as crucial for business executives as it is for adolescents, the rights of adolescents, as older minors, are not nearly as well protected or as well defined as those of adult smartphone users.

Research into and questions about cybersecurity, in the context of children and adolescents, tends to focus on the question of security as protection, where the focus is on such individuals as possible victims of cybercrimes. As children mature into older minors, however, this protection comes, increasingly, at the cost to their privacy.

Social scientists, legal scholars and the community-at-large have long debated the question of a teenager’s right to privacy versus a parent’s or school’s right to know. The introduction of a new technological tool, the smartphone, has altered the nature of that debate and brought to the forefront the intersection of two questions: what is a password and who is an older minor, with respect to control of such a technology.
In order to answer these questions, I will look into the various ways in which the US Supreme Court has attempted to define both concepts. I will attempt to frame each discussion of Supreme Court cases in the context of the classroom, with a general reference to the recent Minnewaska School District case – as that case highlights, at a national level, many of the issues at stake in forming an operational definition of password control for older minors.

This paper will be broken up into three sections, each section answering the following questions: what is the legal nature of a password, what is the legal nature of an older minor and, finally, what kind of operational model might be developed that can best protect the password rights of older minors.

The first section will be a review, from the perspective of Federal Supreme Court Cases that deal with 4th and 5th Amendment rights, in cases of password access under duress for adults engaged in legal proceedings, namely arrest, search-incident-to-arrest and general search and seizure. The second will be a review of US Supreme Court Cases that have set conceptual guidelines for the legal status of an older minor, with a particular emphasis on 1st Amendment rights. Finally, the debate over password control for older minors will be cast in the context of potential criteria for an operational model that attempts to balance between privacy and security for such older minors.

### The Minnewaska School District Case – And it’s National Context

Riley Stratton, a sixth grader in the Minnewaska School District in Minnesota, wrote, in 2011, on her Facebook page that she ‘hated her teacher’s aide’ (ACLU, 2014). Little did she know that her personal opinion would be subject to the scrutiny of school officials, with permanent consequences for her tenure at the school.

In a case that received national attention, the ACLU (American Civil Liberties Union) filed, and won, a 2012 lawsuit against the school district that resulted in a $70,000 settlement for Stratton’s family. (ACLU, 2014)

As lawyers for the case recount:

> ‘In one humiliating ordeal after another, Stratton was subject to a baseless punishment for a comment she made on her own Facebook page, while at home, about a staff member from the school. A short while later she was put through a traumatizing experience when she had her Facebook page searched by school officials, with police present at the search, merely because she allegedly had an online conversation about sex, with a boy, while at home. The whole experience left Stratton distressed to the point where she no longer wanted to attend school.’ (ACLU, 2014)

Stratton’s action, as any brief review of an adolescent’s social life would suggest, is not only not unique, but ordinary. Why then, was the reaction, so extraordinary? How many times in grammar school or high school have we recalled private conversations between friends where opinions of dislike about school teachers and officials took place? Has the right to express such an opinion been lost merely because the medium of its expression has changed? Under what authority, or legal precedent, were school officials acting when they confronted Stratton over what was, ostensibly a semi-public record of opinion, and treated it as a criminal violation?

The short answer, in the case of Minnesota, lies in a 2007 bill on bullying passed by the state legislature. ‘That bill passed the Senate without a single moment of debate, and contained this provision: The policy shall address intimidation and bullying in all forms, including, but not limited to, electronic forms and forms involving Internet use. What kind of policy? How would it enforce off-school activities? How does this infringe of free speech protections? The Legislature couldn’t be bothered with such things, to the consternation of school districts.’ (Collins, 2014)

The vagueness of the provision effectively encouraged school officials to request password access to personal online accounts under the premise that they were addressing acts of bullying or potential bullying, even when there was no suspicion of such acts occurring. The general problem with any form of legislation that refers to mediating acts of bullying is that, much like community ordinances about decency or pornography, it is incredibly difficult to define that term or any term that seeks to impose local community standards as universal laws. At what point does an opinion become an act of bullying? At what point is bullying, as opposed to social play for position within a cohort, an act that becomes so harmful that censure is appropriate? Community standards of decency and pornography, for example, also vary greatly from one place to another. And
although the extremes of violation of such standards might be agreed upon by a universal majority, it is in their minor expressions that the law, and its adjudication, must be questioned and investigated.

The long answer, in the case of Stratton’s lawsuit, lies in a broad national debate about the essence of a password – and about the exact nature of an older minor with regards to privacy and law. Even the resolution of the Minnewaska School District to the lawsuit suggests exactly how difficult this can be, in practice, and how much work needs to be done in developing a consistent operational model of password control for older minors. According to the Star Tribune, a local paper: ‘The school district’s policies have been changed in the wake of this incident. The new rules say electronic records and passwords created off-campus can only be searched if there’s a reasonable suspicion they will uncover violations of school rules.’ (Collins, 2014)

The term reasonable suspicion, however, suffers from the same problem of vagueness as does the term bullying. In addition, the justification for password access for school officials under the concept of reasonable suspicion is just as problematic as the justification for password access requests by law enforcement officials during arrest and search proceedings of adults.

The national context of Stratton’s case highlights the two key issues that are central to the absence of an operational model of password control for older minors: the first is the general absence of a model of password control for adults engaged in legal proceedings and the second is the general absence of a clear definition of the privacy rights of an older minor.

Section I

What is the Legal Nature of a Password?

Although the legal nature of a password, as discussed herein, may have parallel applications in jurisdictions of other countries, the context of this research is limited to the United States. Hence, the legal nature of a password explicitly refers to the legal nature of a password as defined under US Law. In that all laws and federal and state agencies have to comply with the requirement of constitutionality (that is to say that the provisions of any specific law cannot violate the articles or amendments of the US Constitution), the best source for understanding and defining the legal nature of a concept such as a password lies in the place where interpretations of constitutionality occur, namely the US Supreme Court.

There are three amendments (The 1st, 4th and 5th) to the US Constitution that will be reviewed in this paper, as it is the interpretation of these three amendments, in the context of legal proceedings, that has historically been the most significant in the current debate over the legal nature of a password and the definition of an older minor. The amendments, taken directly from the US Constitution (US Constitution, 1787) are as follows:

Amendment I: Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Amendment IV: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Amendment V: No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Within these amendments (as will be discussed), the most significant components that relate to password control are the freedom of speech (Amendment I) and the debate over passwords as ‘protected utterances’, the requirement for warrants upon probable cause (Amendment IV) in the context of search-incident-to-arrest events and the protection against self-incrimination (Amendment V).
Amendment I – Freedom of Expression

Court cases related to password control and freedom of expression will be discussed extensively in the second part of this paper related to the legal concept of an older minor. Beginning with a review of Tinker v. Des Moines, I will look at it and a number of other cases that have attempted to define the scope of First Amendment protection for legal minors.

Court cases that specifically address the issue of password control in the context of First Amendment rights generally do so in the context of what the password provides access to, not the password itself. In other words, First Amendment protection generally concerns what is said, not where it is stored. The debate that will be discussed shortly, about the extent to which a password is more like a lock/key versus an utterance ultimately references the First Amendment, but only in the context that it places one Amendment over the other as being more significant in the case requested and/or demanded access to private information.

Amendment IV – The Search-Incident-to-Arrest Doctrine

Although the issue of warrant access to password protected media is, itself, interesting and complex, the specific case of warrants in the context of compelled password access will only be discussed in the subsequent section about Fifth Amendment rights and the extent to which passwords/passphrases are interpreted as keys or utterances. While the Fourth Amendment generally protects individuals against unwarranted search and seizure, the question of warrantless search and seizure, and its impact on cellphone media, is crucial to the discussion of password control and the legal nature of a password.

The Supreme Court has recognized a number of scenarios (primarily related to arrest events) where police can search people or places without a warrant. (Gershowitz, 2011) The most common exception for warrantless search is classified under the concept of search-incident-to-arrest. Broadly, ‘police are authorized to search the person and his immediate grabbing space to protect against physical danger and to prevent the destruction of evidence. In doing so, police can search in any area or container near the arrestee, including a pocket, a purse, and even a wallet.’ (Gershowitz, 2011) While a number of Supreme Court cases have reaffirmed, in different ways, the general principle of search-incident-to-arrest, the most significant case in the context of password access and cellphone usage is that of United States v. Robinson.

The Supreme Court upheld, in that case, that police officers had the right to open closed containers when searching-incident-to-arrest. The case revolved around the question of whether or not evidence obtained by a police officer (who, during a pat-down, opened a closed container, a cigarette case, which contained heroin) was admissible in court for an arrest related to operating a motor vehicle without a revoked license. (United States v. Robinson, 1973) As a result of the case, the Supreme Court, ‘announced a bright-line rule for searches-incident-to-arrest, permitting police officers to open and search through all items on an arrestee’s person, even if they are in a closed container.’ (Gershowitz, 2011)

In the United States v. Chan and the United States v. Finley, this was extended to wireless devices and cell phones, and the Supreme Court ruled that pagers and cellphones were not distinguishable from luggage, boxes or containers. (Gershowitz, 2011). The Ohio State Supreme Court (State v. Smith) (Gershowitz, 2011), on the other hand, has rejected this interpretation of cell phones as physical containers that are subject to search-incident-to-arrest. A broad variety of rationales and references to both Federal and State Supreme Court cases have resulted in a mixed approach to the question of the cell phone as a physical container.

This legal nature of a password is closely tied to the legal nature of the objects that such passwords protect. As varied results in court cases suggest, a clear classification model is a still a challenge to a field of evidence and personal life that is increasingly virtual and non-tangible. At the same time, password access to a virtual canister such as an email account can be considered far more intrusive than a physical search of an individual’s property. In that email accounts, for example, can house permanent records of entire networks of thoughts, relationships, activities and utterances, it is of utmost importance to regulate warranted and unwarranted access to such archives.

At the same time, we may have to face the fact the concept of search as a right of government itself, whether warranted or unwarranted, may need to be revised as a function of emerging technologies.
translation of the Robinson precedent, whereby cellphones are interpreted as containers, may only be a rough analogy that obscures the very freedoms we seek to protect.

**Classroom Context**

If we transpose the debate over a cellphone as a container, and the implications such a classification has for search-incident-to-arrest scenarios into the context of an educational institutional setting for older minors, we see the same definitional problems arise even, and especially, in situations that are not criminal in nature.

The key question we are confronted with is whether a cellphone (and access to it via a password/passphrase) in an educational setting is more like a locker or more like a wallet. As a locker it is subject to greater scrutiny and control by the school administration than a wallet might be. In other words, a locker is, quite literally, a closed container that is a public object protecting private space. The locker is clearly a part of a school and explicitly exists to further school activities. Therefore, warrantless search of a locker is much easier to both obtain and rationalize for school officials.

However, the same cannot be said of a wallet. Although a student brings a wallet to school, that wallet is very much a private object that does not interact with either the school or other students except to facilitate transactions such as buying lunch or checking out a library book. Where does a smartphone fit in this context? Certainly, school administrators would generally prefer to interpret the smartphone as a type of locker – a container that can be opened upon request and that very much shapes the environment of the school. Privacy and constitutional rights advocates would tend to view the smartphone as something more like a wallet. Not a container exactly, but an extension of a private individual’s body – and the access that body enjoys in social space.

More than anything, these cases demonstrate the fact that the concept of a password cannot, at this point, be separated from the concept of a smartphone itself – and that some convergence in concepts must occur for a clear legal definition of a password to emerge.

**Amendment V – The United States v. Fricosu & Password Access**

The United States v. Fricosu was a federal criminal case in Denver, Colorado that revolved around the question of whether or not an individual could be compelled to reveal an encryption passphrase (password) ‘despite Fifth Amendment protection against self-incrimination.’ (Mataconis, 2012) A hard drive, owned by Fricosu, was encrypted and, as a result, key evidence in a bank fraud case was inaccessible to the prosecution. The prosecution sought to compel her to reveal the passphrase.

The prosecution argued that the password should be treated like a lock-box or key and, therefore, was subject to Fourth Amendment restrictions – in other words, accessible under the provision of a warrant. The defense argued that the passphrase is more like a combination to a safe. ‘While the key is a physical thing and not protected by the Fifth Amendment, the Supreme Court has said, a combination – as the expression of the contents of an individual’s mind – is.’ (Mataconis, 2012) Between the two, classification of a password under the Fifth Amendment provides stronger protection to individuals, because that protection is absolute, whereas Fourth Amendment protection is subject to search and seizure under warrant. The government has generally supported interpretation of a passphrase as being legally equivalent to a lock-box or key. ‘Encrypting all inculpatory digital evidence would serve to defeat the efforts of law enforcement officers to obtain such evidence through judicially authorized search warrants, and thus make their prosecution impossible.’ (Kravets, 2012a)

On the surface, the court (which ruled in favor of the prosecution) and companies with access to password encrypted information (such as the major email, social media and networking companies) tend to favor a classification of a passphrase as being more of a lock-box or key – and therefore subject to access via warrant. An individual who know Google’s law enforcement procedures stated that ‘the company will provide assistance to law enforcement agencies seeking to bypass screen unlock patterns, provided that the cops get the right kind of court order.’ The company insists on an ‘anticipatory warrant, which the Supreme Court has defined as a warrant based upon an affidavit showing probable cause that at some future time, but not presently, certain evidence of crime will be located at a specific place.’ (Soghoian, 2012) Although limited in its
scope, with respect to other categories of warrants, the tendency in classification is pushing towards a model of the password/passphrase as being legally equivalent to a lock-box or key, and not an utterance.

However, not all courts agree with this interpretation, even though it clearly favors security over privacy and the right of the government to know versus that of the individual to protect themselves against incrimination. At issue is not just the information that might be obtained through the disclosure of such a password/passphrase, but the fact that capability to access might be equated with culpability. A recent case in the US District Court in Eastern Wisconsin (Jeffrey Feldman v. Appellate Court of Wisconsin) (Weebly, 2013) has ruled in favor of the password as protected under the Fifth Amendment under this reasoning. The accused in the case, objected to being forced to give up the password by asserting that, 'by decrypting the contents, he would be testifying that he, as opposed to some other person, placed the contents on the hard drive, encrypted the contents, and could retrieve and examine them whenever he wished.' (Techdirt.com, 2013) In other words, just as meta-data can provide, through a footprint of digital crumbs, crucial information about the content of communication without disclosing that communication, so, too, can the demonstration of the knowledge of a password provide incriminating information about the nature of data that is encrypted. The court argues, effectively, that, because knowing a password can be construed as being responsible for the data that the password protects, one should not be required to provide such a password – as doing so violates the Fifth Amendment protection against self-incrimination. ‘Feldman’s act of production, which would necessarily require his using a password of some type to decrypt the storage device, would be tantamount to telling the government something it does not already know with reasonably particularity—namely, that Feldman has personal access to and control over the encrypted storage devices.’ (Techdirt.com, 2013)

The Electronic Frontier Foundation filed an amicus brief in the afore-mentioned case of the United States v. Fricosu using the same logic. ‘Decrypting the data on the laptop can be, in and of itself, a testimonial act — revealing control over a computer and the files on it,’ said EFF Senior Staff Attorney Marcia Hofmann. ‘Ordering the defendant to enter an encryption password puts her in the situation the Fifth Amendment was designed to prevent: having to choose between incriminating herself, lying under oath, or risking contempt of court.’ (EFF, 2011)

Slight variances in the concept of the legal nature of a password (key versus utterance) are having a profound impact on civil liberties in a digital era. As the court cases reveal, the issue has not been decided at this time. Leaning towards the password as key may lead to a more secure society, but will invariably come at the expense of privacy. At the same time, interpreting the password as utterance may allow certain people to commit serious crimes and go free because the evidence against them (present only in digital form) may be inadmissible in court and/or unaccessible to law enforcement.

Classroom Context

The classroom context for older minors presents unique challenges in the case of Fifth Amendment rights. The majority of incidents that occur within school grounds are not incidents that warrant arrest and, therefore, are not subject to Fifth Amendment protections in the traditional sense of the concept. Rather, they are most often variations on self-incrimination or group incrimination demands on behalf of school teachers and/or administrators where suspicious, but not criminal activities, occur. Let us imagine, for example, the case of a student suspected of cheating on a test. The teacher believes that a friend sent the answers via text message during the exam. Does the teacher and/or the school have the right to search the friend’s smartphone to review the text messages? Or does the friend have the right to protect against self-incrimination (as a conspirator in the act of cheating on the test) or incrimination of a friend? Even more to the point, let us assume that the teacher already confiscated the smartphone in question, but does not have password access to it. Does the teacher have the right to request the friend's password? Does the friend have the right to deny the request on the basis of Fifth Amendment protection, even if the issue at stake is not a criminal issue?

Judges and lawmakers are divided on this issue in the context of admissible evidence in court (Sengupta, 2012) It should come as no surprise that this division in perspective extends to school districts and school administrators across the United States. The questions in the example above are not meant to be answered...
here. Rather, they are meant to provide insight into how sensitive and particular this specific type of password controlled interface can be in maximizing the pursuit of happiness of both school officials and students.

**Section II**

**The Constitutional Rights of Older Minors**

One of the key challenges that educational institutions face in their responsibility for both the welfare and development of older minors is the balance between privacy and security. While no one would argue that it is in the interest of all students for the school to be able to routinely check the contents of lockers to regulate and restrict the presence of weapons on school grounds, it is harder to argue that schools have the right to access students’ social media accounts to regulate and censure opinions about other students or teachers.

And yet, schools, like any institution of power, will routinely attempt to push the boundaries of their control, just as school administrators did in the Minnewaska School District. The fact that such intrusions into privacy are accepted and tolerated by the members of a school community does not, however, mean that they are legal – or, in more specific terms, that they respect the legal rights and privileges of older minors.

A number of significant Supreme Court Cases have ruled on the constitutionality of institutional denial and control of certain rights with respect to older minor in such settings. The most significant among them, in the context of this discussion are: In re Gault (1967), Tinker v. Des Moines (1969) and New Jersey v. T.L.O. (1985). The cases above are cited as a reference for establishing a baseline for the general constitutional rights of older minors, with the specific intention of answering the question: who is an older minor? Only when this question has been addressed can the question of password rights for older minors be considered.

**In re Gault (1967)**

This Supreme Court Case in 1967 established a significant historical precedent about teenagers, namely that teenagers have distinct rights under the Constitution – and are not merely the property of their parents. (Jacobs, 2008) Gerald Gault was a 15-year old in Arizona who was on probation and was arrested and taken to a Children's Detention Center in Arizona after being accused of making an obscene phone call. Repeated denial of due process during detention, arraignment and judgment proceedings were contested by Gault's parents. They filed a petition for a writ of habeas corpus that was denied repeatedly at the state court level. (In re Gault 387 U.S. 1, 1967) The U.S. Supreme Court heard the case, however, and used it as a landmark case to ensure that rights of due process are not limited to adults. The Court wrote specifically that the 'procedural rules which have been fashioned from the generality of due process are our best instruments for the distillation and evaluation of essential facts from the conflicting data that life and our adversary methods present.' (In re Gault 387 U.S. 1, 1967) Had Gault been a legal adult, he would have been afforded rights of due process. The Court determined that 'while there are legitimate reasons for treating juveniles and adults differently, juveniles facing an adjudication of delinquency and incarceration are entitled to certain procedural safeguards under the Due Process Clause of the Fourteenth Amendment.' (In re Gault 387 U.S. 1, 1967)

The significance of the case was not only in its specific protection of due process for juveniles, but in the generalizability of protection of rights afforded juveniles under the Constitution. In effect, In re Gault upheld the idea that older minors are not the property of their parents and, as such, are entitled to the protections and rights of legal adults. This case opened the door for future challenges to infringements on the rights of older minors.

**Tinker v. Des Moines (1969)**

Three public school students (aged 13-16) in Des Moines, Iowa, were suspended from school for wearing black armbands to protest government policy in Vietnam. (Tedford, Herbeck, 2009) The Des Moines School Board was sued and the District Court sided with the School Board and 'upheld the constitutionality of the school authorities' action on the ground that it was reasonable in order to prevent disturbance of school discipline.' (Tedford, Herbeck, 2009) The case was appealed and, ultimately, was reviewed by the U.S. Supreme Court.
The Supreme Court cited two precedents, in its majority ruling, that have been used ever since to protect First Amendment rights of students on school grounds. The first was that ‘First Amendment rights are available to teachers and students, subject to application in light of the special characteristics of the school environment.’ The second was that a ‘Prohibition against expression of opinion, without any evidence that the rule is necessary to avoid substantial interference with school discipline or the rights of others, is not permissible under the First and Fourteenth Amendments.’ (Tedford, Herbeck, 2009)

Building on In re Gault, the Supreme Court upheld the principle that an older minor’s constitutional rights are not abridged or suspended upon entering a school building. It is important to point out, however, that, just as in the general community for legal adults, first amendment protection is not an absolute right. Rather, it is a relative right mediated by the opportunity for imminent harm or disruption that its exercise might generate. The classic example of this limitation in practice is that of yelling fire in a crowded theater. Yes, it is an utterance. Yes, it is speech. No, it is not protected, because this specific utterance in this specific case is highly likely to cause bodily injury and harm to others. The same reasonable tenant holds in discussing the legal rights of an older minor in entering a school building. Such a minor has no right to, for example, convey utterances in a public forum where those utterance might cause immediate harm to others.

It should be remembered, however, that the issue under discussion, that of password control for older minors, is most significant when its infringement is not most harmful, but least harmful. For example, a school official’s request to see a student’s Facebook account to verify the whereabouts of another student accused of a serious crime, such as murder, is not at issue. For such an intrusion into privacy comes with a clear understanding of the security of all students being at stake. However, when a student expresses an opinion of hate or disgust towards a school administrator (as happened in Minnewaska) and is then punished for it, the issue comes directly to the foreground. More uniquely so in the case of schools than other places, in fact.

In another case, that of Keyishian v. Board of Regents, Mr. Justice Brennan, speaking for the Court, said: ‘The vigilant protection of constitutional freedoms is nowhere more vital than in the community of American schools. The classroom is peculiarly the marketplace of ideas. The Nation’s future depends upon leaders trained through wide exposure to that robust exchange of ideas which discovers truth out of a multitude of tongues, [rather] than through any kind of authoritative selection.’ (Tedford, Herbeck, 2009)

The lesson we can draw from Tinker v. Des Moines is not simply that the First Amendment rights of older minors are protected in schools, but that schools have an unusual and extraordinary responsibility to shape a culture that fosters a true marketplace of ideas. Not only should schools seek to ensure that they do not overstep their zealousness for security in the name of student protection, but, if we interpret the reasoning of the court correctly, schools should undertake to be excessively permissive in their students’ expression of first amendment rights. The fact that this is not the case, and appears to be moving in quite the opposite direction with the rise of school monitoring and vigilance of online activities that occur outside of school is not only troubling but must be systematically guarded against.

At the moment, the Supreme Court is resisting moving away from the Tinker v. Des Moines precedent, despite the fact that its relevance in a digital age is being increasingly criticized. (Kravets, 2012b) Specifically, it has refused to hear cases that challenge the applicability of Tinker v. Des Moines in the context of online media. The leading case that the Court has refused comes from the 3rd U.S. Circuit Court of Appeals, which ‘ruled last year that local Pennsylvania school district officials over-reacted and breached First Amendment rights of a junior high school student who ridiculed the principle on-line while using an off-campus computer.’ (Kravets, 2012b) The reason the Circuit Court has petitioned the Supreme Court is that the same Circuit Court, with different judges, approved the ‘10 day suspension of a 14 year old student who mocked the principal with a fake Myspace profile (which suggested that the principal was a sex addict and pedophile).’ (Kravets, 2012b)

The problem is that both rulings cite Tinker v. Des Moines as their precedent. This internal conflict between judges in the same Circuit Court mirrors the broader problem of the applicability of Tinker v. Des Moines in a digital age. The fact that the Supreme Court does not want to hear the case may be that it does not yet feel ready to create a landmark precedent on a technology platform that is so new and so rapidly emerging. Doing so to soon may create dangers for both sides: either curtailing First Amendment Rights or endangering the security of students.
Not hearing the case, or a case like it in the near future, may do even more damage, however. A lack of consensus on the constitutional protection afforded older minors in educational institutional settings may inhibit their communications and utterances – and ultimately negatively impact the future leadership of the country.


Two New Jersey high school freshmen were caught smoking cigarettes in a school bathroom. The assistant vice-principal asked one of the students TLO to hand over her purse to determine if there were, in fact, cigarettes in the purse. ‘The officials discovered cigarettes, a small amount of marijuana, and a list containing the names of students who owed T.L.O. money. T.L.O. was charged with possession of marijuana.’ (Oyez, 2014) TLO countered that the school violated her Fourth Amendment rights by conducting an ‘unwarranted’ search of her purse. The decisions between courts, on appeals, went back and forth and the case finally landed in the U.S. Supreme Court. The Court ruled 6-3 in favor of the school. Justice White, for the majority, stated, ‘Our consideration of the proper application of the Fourth Amendment to the public schools, however, has led us to conclude that the search that gave rise to the case now before us did not violate the Fourth Amendment. Accordingly, we here address only the questions of the proper standard for assessing the legality of searches conducted by public school officials and the application of that standard to the facts of this case.’ (Oyez, 2014)

The logic of the ruling, and the admissibility of evidence obtained through unwarranted search follow a logic similar to that of probable cause – in looking for cigarettes, a school administrator stumbled upon something where the cigarettes would have been, but weren’t cigarettes. The Supreme Court employed, in the TLO case, support for extension of the concept of search-incident-to-arrest to situations that do not merit arrest, but do impact older minors.

The question we are left with, after the TLO case is: how does the case alter or change or view of an older minor? The case appears to define an older minor as having fewer rights than a legal adult, in that the doctrine of search-incident-to-arrest can be extended to situations of probable cause that violate school rules alone. But is that always true? The TLO case reveals more questions than answers. It tells us more about what an older minor is not (a legal adult) than what an older minor is.

**Section III**

**Towards an Operational Model of Password Ownership for Older Minors**

As the decisions of the Supreme Court indicate, neither the concept of a password, nor that of an older minor has been established within the parameters of a category schema that is applicable in all cases to all instances of password request. A simple map of variances in warrantless cellphone search powers in the United States illustrates the complexity of the problem. Three states require a warrant to search a cellphone. Twenty states don’t require a warrant to search a cellphone. The rest have not ruled decisively on the matter. (Hill, 2013)

Until the Supreme Court either has the opportunity and decides to hear a case that specifically addresses the issue of the rights of an older minor to absolute password control for online personal devices, the legality of such ownership for older minors will be in dispute. The Court decisions, to their credit, however, also highlight the complexity of balancing security and privacy in the context of powerful online personal tools that significantly stretch any individual’s capability to exercise power at a distance and to archive or access significant data about personal and private life.

As personal online tools become both more powerful and more pervasive, however (such as with the emergence of wearable and embedded online devices) the need to protect the password rights of older minors will only increase. It is very easy to imagine a not-too-distant future scenario where a school might ask a potential student athlete to provide access to a password encoded wearable microchip that contains sensitive information about the student’s DNA that might be used against the student to make life-changing decisions about athletic status. Or a scenario where personal records from wearable eye-wear devices might be confiscated by school officials without warrant or consent.
The trend towards increasing potential exposure to private data and increasing embeddedness of personal online devices suggests that some sort of model to regulate behavior needs to be developed. The testing and full assessment of such a model is beyond the scope of this paper, but, given the complexity of the current debate – and its inability to provide conclusive categorical definitions for either a password or an older minor, I believe it makes sense to discuss the general parameters of what an operational model of password ownership might look like.

Let me explain what I mean by operational model as opposed to legislation. The ultimate decision by the Supreme Court to define (or not define and leave in the hand of State Supreme Courts) the issue of password control for older minors will hopefully result in legislation that balances the school’s need for security with the older minor’s right to privacy in some way.

In the absence of legislation, an operational model for authoritative decision-making may be helpful in determining which side of the proverbial legal fence a given situation falls. The operational model that I am proposing is one that uses the baseline of entrusted and legal private behaviors of legal adults that older minors can and do (sometimes, but not always) legally also engage in, wherein that engagement affords them the same rights to privacy that legal adults enjoy. As such, the question of password ownership for older minors than becomes explicitly and only a question of password ownership for legal adults. These two behaviors fall under the broad categories of consent laws and motor vehicle laws.

**Minor Consent Laws**

Over the past 30 years the ability of legal minors (largely defined as being age 12 and older) to consent to a broadening array of health services has expanded drastically. (Guttmacher, 2014) ‘Nearly every state permits minor parents to make important decisions on their own regarding their children. In sharp contrast, the majority of states require parental involvement in a minor’s abortion.’ (Guttmacher, 2014) Although there are variances among states, minors can access a broad array of health services, without parental consent. These includes: contraceptive services, prenatal care and adoption for minor parents. (Guttmacher, 2014)

The preference for treatment of older minor parents as legal adults highlights the complex status of an older minor and illustrates the contextual nature and fluidity of that definition. Why would a 14 year old who bears a child suddenly enjoy privacy privileges in health services reserved for an adult, but not enjoy privacy privileges in conversations through social media at the same level? Why are some teenagers who commit capital crimes tried as adults, and others are not?

Despite enormous differences in consent given to older minors, one fact stands out: consent, and the extension of legal adult status to older minors is directly related to older minors doing things that legal adults do. In this sense, one aspect of an emerging precedent is clear: when older minors use passwords (and by extension the devices those passwords protect) to perform functions of legal adults than they should be increasingly afforded the status of legal adults.

**Permits & Driving Licenses**

The fact that older minors can possess permits and driving licenses before the age of 18 in many US States may provide a different insight into the construction of an operational model of password control that is, in many ways, analogous to the enjoyment of legal adult privileges granted to older minors in making decisions about health services when such services concern the status of older minors as parents (or would-be parents).

Driving requires a license or permit because of the enormous safety issues involved in someone handling a motor vehicle. At the same time, however, I would argue that driving confers an ancillary benefit on an older minor that is directly related to the issue of password control: that of implied privacy. Although parents, and technology companies, will inevitably come up with more and more ways to track automobiles and their usage, the driving license confers a unique privilege of privacy on an older minor. In effect, the license or permit is the right to travel on one’s own – presumably within certain constraints (related to time of day and in-state usage). This right is also a right to have a private life. If an older minor can drive, than society has effectively bestowed on that minor a distinct and private existence – an existence that should also be protected in digital form.

DOI: 10.5604/23920092.1134790
Conclusion

Developing an operational model of password control for older minors that is contingent on older minors conducting activities of legal adults does not resolve the password definition issue. Rather, it leaves us at a point with more apparent questions than answers.

Ultimately, I believe the only operational model of password control for both legal adults and older minors that will work in the future will be one that pushes towards a completely different construct – that of 'bionic' or 'hyper' citizenship. This concept is also discussed under the idea of a 'cyborg bill of rights'.

Without getting into the details, let us imagine the following scenario (which most likely will be possible within a few years). A blind individual is given an artificial eye that is actually an advanced computer. The chip, embedded inside the eye directly can record what is seen and those recording can be played back by the individual as a form of private memory. This individual is arrested and alleged to take part in a crime. Does a court have the right to 'connect' to that chip and force the individual to make public the record of what that artificial eye has seen? Or, is that artificial eye now considered an aspect of the person – and, as such, protected under the 5th amendment?

Given the power of smartphones to record and capture, in digital form, the real and private world of individuals, shouldn't we perhaps treat the smartphone the same way that we might treat such a cybernetic apparatus – as a direction extension of the body of the citizen? In other words, do smartphones represent the last piece of technology that is still separate from us (and therefore subject to ordinary scrutiny of existing law) or do they represent the first set of technologies in a new form of bionic or cybernetic citizens?

Will the protections and legal status of bionic citizens be different? 'A bionic ethic,' according to David Channel, 'must take into consideration both the mechanical and the organic aspects of the cybernetic ecology in order to maintain the system's integrity, stability, diversity, and purposefulness. Neither the mechanical nor the organic can be allowed to bring about the extinction of the other.' (Channel, 1991. 154) How different must different become in order for laws to change?

Chris Gray has proposed that only a new cyborg bill of rights will adequately protect such bionic citizenship. (Gray, 1997) He has enumerated a number of rights, such as the freedom of electronic speech, the right of electronic privacy and the freedom of personal information (Gray, 1997). The question that is, I believe, left to answer is not one of creating a legal line that defines both a password and an older minor. An operational model of password control for older minors must persist, principally (I believe) through the mechanism of graduated legal behavior in older minors, until a new model of bionic citizenship emerges. Are smartphone users the last of the age of computers, or the first of the age of cyborgs?

References


