Social Education 76(4), pp 217–220

Teaching Privacy in the Twenty-first Century

Odette Edbrooke and Meg Leta Ambrose

What would Benjamin Franklin's Facebook page look like? Would he be "friends" with William Pierce, James Madison, or Alexander Hamilton? Would there have been a separate Facebook group for the framers of the Constitution, where they would have posted comments on the wall regarding the different stipulations that needed inclusion in the document? Talk of revolution took place in quiet corners of taverns along the East Coast, but would the text messages between the Sons of Liberty have been viewed as equally treasonous? If e-mail, web pages, Facebook, and other digital content had existed at the time the framers addressed the rights of citizens in the newborn nation, this could have affected the language of the Bill of Rights. Would the First Amendment, which prohibits Congress from enacting legislation "abridging the freedom of speech, or of the press," have been reworded? Would information on the web have been included in the list of things protected against unreasonable search and seizure? If Benjamin Franklin and his Facebook friends had been aware of the technology that is ubiquitous in the United States today, what would be different in the very document that governs American society?

Questions like these can encourage our students to view the eighteenth century in a new light and to understand the contemporary relevance of the Constitution and its Amendments. Today's students are fascinated by technology and its applications. We believe that teachers have a great opportunity to build on this interest as they teach about the Constitution and its Amendments.

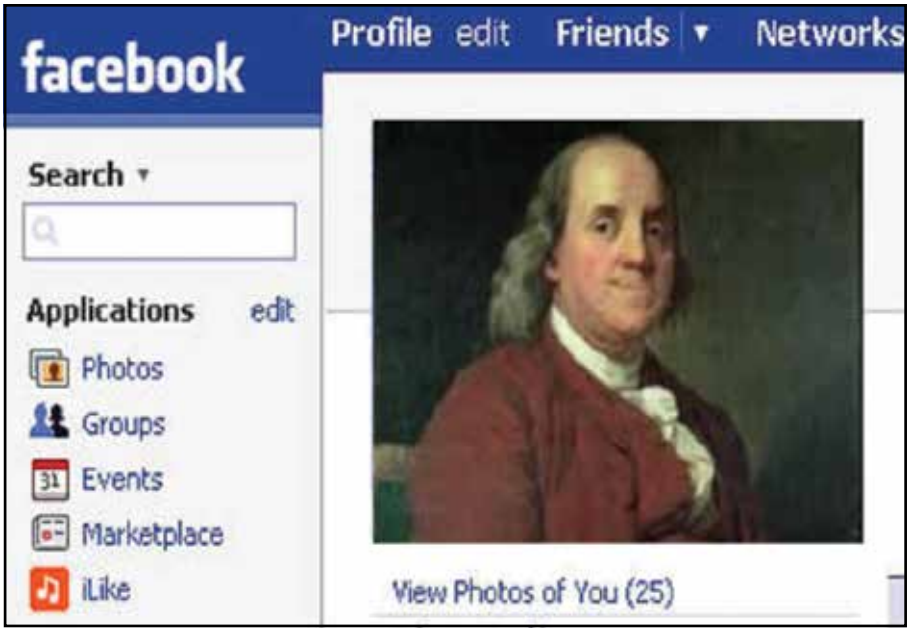
Based on the English Bill of Rights of 1689, the United States' Bill of Rights outlines the inherent rights and privileges that every citizen should be guaranteed. Crawling out from under the tyrannical rule of King George III, the revolutionaries, thinkers, and political leaders of the newly born United States were desperate for an explicit outline of the inherent rights advocated by the eighteenth-century Enlightenment. They achieved their objectives with the Bill of Rights, which consists of the first ten amendments to the Constitution.

The Bill of Rights guaranteed freedom of speech, press, religion, and assembly. It offered protections for citizens to exercise their voice actively in government or to "redress their grievances." It granted the right to bear arms, and citizens were shielded from having to quarter troops in their homes. The Fourth Amendment provided that search and seizure was no longer a carte blanche luxury of law enforcement, but rather a process that required a rationale and list of expectations to justify the searching of citizens' persons and properties by law enforcement officials. The guidelines for the rights of the accused were laid out to avoid any abuse of the legal system.

Society and culture have changed rapidly over the last 200 hundred years, and in the Digital Age, that change has accelerated. The law has also evolved dramatically and is continuing to evolve in the face of emerging technology. The new network society offers an opportunity for students to learn about the evolution of the law as it relates to the technology that subsumes their lives. Digital natives and the generations that follow are born into a culture with pervasive technology; it has altered their perceptions of their freedoms and how these freedoms fit into contemporary life. It is imperative for students to understand freedom of speech and privacy issues in these updated contexts, which have arisen hundreds of years after the first and fourth amendments were written. How do these amendments apply to *their* freedoms and *their* rights?

The Fourth Amendment reads

> 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.



Benjamin Franklin has multiple Facebook pages online today, posthumously written in a medium seemingly unfathomable in the 18th century. The role of technology has not only tested the interpretation of the Bill of Rights, but has also altered the way it needs to be taught in civics classrooms.

The language of this Amendment and others has been interpreted to establish a right to privacy: the Constitution protects private aspects of life from unwarranted government invasion. In practice, the issues arising from this concept can be incredibly complicated. They have become even more so in these days of technological immersion, as a result of the dramatic innovations of the last 20 years.

This year's incoming high school freshmen were all born in the late 1990s. A period of more than 200 years of technological advances separates the Framers from the smartphone. Most of this year's freshmen were born in 1997, 1998 or 1999—a very brief period of time dotted with events like the spread of instant messaging, a Y2K scare, the development of high speed bandwidth, reliance on emails, the evolution of smartphones, and ubiquitous connectivity. These students have known almost nothing but pervasive technology and total access. For many of them, dial-up is an unidentifiable sound.

This new breed of high school student sits in Civics or Government courses nationwide listening to traditional lectures on the Bill of Rights. How does that classroom need to change to reflect today's issues, particularly when addressing the First or Fourth Amendments? How should social studies teachers address the question of privacy, when the Fourth Amendment reference to "papers" could represent digital versions and copies of intellectual properties? Is a posting on Facebook considered a private paper? Can an employee be fired because of something he or she posted on a personal page at home, which is public on the Internet?

In the classroom, it is important to raise these very questions. To do so requires content that goes beyond the normal range of social studies content. In addition to redefining and interpreting many of the social studies themes related to Fourth Amendment rights, some technology content should be taught as well.

As part of the University of Colorado's Engaging Computer Science in Traditional Education (ECSITE) program, we have designed a set of lessons to challenge students' beliefs and understanding of privacy, and bring to light the differences and issues that are the product of the twenty-first century. This allows the class to explore different concepts of privacy such as seclusion, control, access, and secrecy. We bring up-to-date and relevant topics into the curriculum, while introducing underrepresented groups such as women and minorities to computer science.

When teaching these, or any other lesson plans, on the impact of technology on privacy, the ambiguity of certain words necessitates group discussion of their application in the twenty-first century. These words include, but are not limited to: private, public, property, papers (as used in the Fourth Amendment), bodies, effects, violation, expectations, and probable cause. The easiest way to start is by asking whether Facebook pages are private or public? To whom? How do the privacy settings factor into the analysis? How about the password?

The Lessons

Both of the following lessons are detailed at length on the ECSITE website (**http://ecsite.cs.colorado.edu/units/civics-and-social-sciences/**), including all slides and detailed lesson plan outlines. In the first lesson, "Updating Political Values," an introductory discussion should be held in which students examine ambiguous terms, followed by an explanation of the differences between the concepts of Originalism and the Living Constitution. The students should then be asked to analyze a number of current privacy issues involving emerging technology and debate over what is private, what is public, what is disclosure, who should have access to your information, and under what circumstances?

The following discussion involves creating distinctions and parallels between the application of the Fourth Amendment to eighteenth century and twenty-first century problems; the students can also address the intentions of the framers of the Constitution. The three comparisons below can be pre-

sented to the class through a PowerPoint, guided by the teacher to explain any technological differences that may be confusing.

1. What would the Founding Fathers say about privacy rights in mail? Does a citizen have privacy rights in the information held in the recipient's name, address, sender information, and contents of envelope? What would they say about the privacy of an email and the correlated sender information, IP address, account location, and subject line? Should it matter that one is transmitted by the government and one by a company? What are the real differences between mail and email?

2. What would the founders say about the privacy of GoogleChat vs. the privacy rights in a phone conversation? Both involve intimate information and can be intercepted without trespassing into a home by law enforcement, but chats are stored on Google servers, can be set to private, and require a password. Who should hold the rights to the chats: Google or the consumer? What does that mean for the Fourth Amendment application?

3. What is the difference between a traditional police stakeout and tracking a suspect by attaching an electronic location surveillance to his or her vehicle (geo-tracking)? In both instances, the suspect is unaware of the surveillance, but the traditional form of keeping tabs on a suspect is limited to monitoring from public places and by human and financial resources. Should law enforcement need a warrant for one, both, or neither?

The following scenarios involve non-governmental privacy issues and are given to students to discuss in small groups. Each group can be given a different scenario to then present to the rest of their peers.

- Should a student receive school consequences if he or she broke the school code of conduct, but the evidence was found in a photograph on Facebook?
- Should a potential employer be able to use information found on a social media network to determine the qualifications of a job applicant?
- Should colleges and universities have access to social media profiles in order to prevent their students from posting inappropriate material that can be seen by recruits and potential students?
- What needs to be protected when Google takes images for Google Earth? For instance, should windows be blurred out in the image? What about license plate numbers?
- When should an individual be notified that her or his images are being used in Google Earth?
- How should the "tagging" of others in a photograph be regulated? Should the subject of the photograph be held responsible for the content if he or she was not the one who made it public?

The next lesson, "Anonymity and Privacy: Encryption and Decoding in Digital Speech," introduces anonymity as an element of the First Amendment and privacy. Question whether students see the value of anonymity, whether they change their behavior if someone is watching them, and whether "demasking" online users is a good or bad idea. Once students are comfortable with these notions, introduce code and architecture as a form of controlling information. A helpful analogy to the way code restricts online use is the way a fence restricts activity around a house. How can code be used to encourage expression and protect privacy?

If vulnerable information must stay secret, encrypting the information may be the best way to protect it, instead of relying on trust or the law. Encryption supports the distinction between public and private material, even though all information is transmitted over a public space. When locked with certain types of encryption, information is demarcated with an expectation of privacy. It is important to understand how that demarcation is created and broken.

Begin with a Power Point (one is provided on the ECSITE website). Slides include a distinction between civil and criminal actions--the difference between law enforcement invading privacy and non-governmental individual or group invading privacy. These slides will promote further discussion of the rights of anonymous communication and the rights to access information, but should be adapted to fit the classroom.

The presentation should then lead into an explanation of the ciphers. A plaintext, such as "my dog barks," is encrypted with the cipher text, such as "nz eph cbslt." This is a simple cipher shift. The plain text is built from the alphabet and the cipher text is built from the alphabet starting with the letter B instead of A; A is represented by B, B as C, and Y as Z in the cipher text. The recipient needs to know the cipher in order to break the code. All encrypted messages can in theory be broken by a brute force attack, some requiring an incredibly powerful computer that would attempt every possible cipher until stumbling on the correct one.

Public Key cryptography is a foundation for safe Internet communication. It is a system that requires two keys, one public and one private. One will encrypt the plaintext and one will decrypt it, but neither will do both. The following exercise demonstrates the system in a way that can be easily understood.

1. Pick five students to stand in a line in front of the room.

2. Pick one student on the end to be the "sender."
3. Pick the student on the other end to be the "recipient."
4. The middle student is the "bad guy."
5. A bag of candy is the "message."
6. Provide a tackle box as the container for the message.
7. Have the sender put the message in the tackle box.
8. Have the sender lock the box ("encrypt the message").
9. Send the message "through the Internet" by having the sender pass the box down the line of students.
10. Check to make sure the bad guy cannot open it.
11. Have the box received by the recipient.
12. Can the recipient open the box with the sender lock on it? No.
13. Have the recipient put an additional lock on the box, so there are now two locks securing the message, but no key has been transferred.
14. Pass the box back through the Internet to the sender.
15. Can the bad guy in the middle of the transmission open it with the two locks? No.
16. Continue to send the box to the sender.
17. Sender takes her or his lock off using the key that has remained in her or his possession.
18. Sender sends the box back to the recipient who can now unlock the box because only the recipient lock remains and he/she holds the key.

Once students understand the Public Key encryption, give students three different codes to break. Each student gets a reward once they break one of the codes. This can also be done in groups. Three students per group works well.

Conclusion

In each lesson, it is important to remind students about the perspective of the framers. What were their priorities? In post-revolutionary America, what regulations did they perceive as necessary for the United States? By putting these questions in the context of the technological issues that are currently challenging the U.S. legal system, we can provide students with a firm grasp of the rights that are relevant to them.

Odette Edbrooke *is a social studies teacher leader in the Boulder Valley School District, where she teaches at Fairview High School. She also served as a Teacher Mentor in the University of Colorado's program Engaging Computer Science in Traditional Education (ECSITE), sponsored by the National Science Foundation. She can be contacted at* odette.edbrooke@bvsd.org. **Meg Leta Ambrose** *was a Graduate Fellow in ECSITE and is a doctoral candidate at the ATLAS Institute at the University of Colorado, Boulder.*