SECTION III.

Tips for parents looking to protect their student's privacy

Children and their parents are under intense pressure to engage with technology at home and at school. Whether children are voluntarily using personal social media or assigned to use applications (apps) and online programs by their teachers, they are sharing more and more details of their lives online. You may feel like the genie is out of the bottle, but it's not too late to take simple steps to protect your children's privacy. Give these suggestions a try!

Tips for home

RESIST THE URGE yourself to share everything with everyone. Before posting intimate photos or details about your children's life on social media, consider the long-term implications of sharing this information so widely. One study found that children resent their parents posting pictures of them on social media without their consent.[1] Another study found that the average parent in the United Kingdom shares nearly 1,500 photos of their children before they turn five.[2] Talking to your children about what's appropriate for you to post is also a great way to jump-start important conversations about their own social media behavior.

It's estimated that 81% of the U.S. population maintains at least one social network profile.[3]

SET BOUNDARIES with your children. Discuss what information is appropriate to share online and what is not. Encourage them to ask permission from their friends before posting or sharing pictures of their friends with others.

A recent study revealed that "[t]he same brain circuits that are activated by eating chocolate and winning money are activated when teenagers see large numbers of 'likes' on their own photos, and teenagers are definitely influenced by their online 'friends,' even if they barely know them."[4]

INSTALL AD-BLOCKERS on personal laptops, devices, and phones your children use at home. For example, Privacy Badger,[5] or a combination of AdBlock[6] and Ghostery,[7] allows websites to load faster and blocks ads that may contain malware or other viruses. These programs can also prevent companies from tracking and profiling your children.[8]

PLACE A STICKY NOTE or non-stick adhesive bandage (e.g., a Band-Aid) over the camera lens on your and your children's devices to prevent hackers from turning them on. Facebook founder Mark Zuckerberg and FBI Director James Comey do it![9]

BEFORE DOWNLOADING FREE APPS, consider that if an online service or product is ostensibly offered for "free," the real price you pay is often your children's information, to be exploited for marketing or other commercial purposes. Encourage your kids to ask your permission before signing up. If they're under age 13 and they are providing personal information, this is legally required under the Children's Online Privacy Protection Act (COPPA) when the website is child-directed. For more information on COPPA, see Section II.

Give yourself an added layer of protection by using the Electronic Frontier Foundation's "HTTPS Everywhere." Learn more at www.eff.org/https-everywhere

CONSIDER CREATING A NEW EMAIL ACCOUNT — with no real name or other identifying information attached — for signing your children up for apps or online accounts.

TEACH YOUR CHILDREN to create usernames and passwords for online accounts

without using any of their personal identifying information like their names, dates of birth, student number, pet name, or school names.

Help your child create strong passwords! Try using an acronym for something your child will easily remember, preferably a full sentence. Use combinations of upper- and lower-case letters, numbers and symbols. For example, the sentence "I love the FIFA World Cup video game" could be expressed as "I<3tFIFAWCvg."

TERMS OF SERVICE and privacy policies are often deliberately long, complicated, and hard to understand. Use the section below, What to look for in terms of service and privacy policies, to scan the policies and terms of any apps or online programs used by your children. If you see any of the red flags from that list, do not allow your child to use them.

Tips for school

ASK YOUR CHILDREN'S TEACHERS which classroom apps and online programs will be assigned throughout the year, and what personal student information each app collects. Ask if these programs have been approved by either the district or state for privacy and security protections and compliance with state and federal laws. For a list of questions to ask your teacher, see Section V and Appendix D.

Education technology is big business! In February 2015, the Software and Information Industry Association (SIIA) estimated the value of the PreK-12 educational software and digital content market at $8.38 billion.[10]

ENCOURAGE YOUR CHILDREN'S TEACHERS and school to resist using non-essential classroom apps and online programs whenever possible. Consider opting your children out of using insecure or excessive apps and online programs.

ASK YOUR CHILDREN'S TEACHERS if they can create accounts without using their students' real names, and/or refrain from disclosing any student information not needed for the use the app or online program.

Why are some classroom apps free and what does this mean for your child's privacy? Technology can be a tool to enhance student learning, but it can also be expensive, which is why free software and classroom apps are so appealing to schools and teachers. But as the old saying goes, "nothing in life is free." If the school or district is not paying for the classroom app or online program, the company is most likely profiting from your child's information in some other way.

DON'T ASSUME the privacy policies of apps or online programs assigned to your children — especially free ones — have been sufficiently vetted by their teachers. Educational or classroom apps may not respect student privacy any more than other apps.

SCAN THE TERMS OF SERVICE and privacy policies of any classroom app or online program your children are assigned. If you see any of the red flags described in the section below, approach the teacher or principal with your concerns.

ASK YOUR PRINCIPAL if the school keeps personal student information in the "cloud," and if so, if there is a contract to bar the vendor or operator from selling the information, redisclosing it to others, or using it for non-educational purposes. Ask if the information is properly encrypted in transmission and at rest.

A 2010 study by Fordham Law School found that "95% of districts rely on vendors for a diverse range of functions including data collection and mining related to student performance, support for classroom activities, student guidance, data hosting, as well as special services such as cafeteria payments and transportation planning."[11]

TALK TO YOUR HIGH SCHOOL CHILDREN about military recruiters who may be visiting their school campus. If your children are not considering enlisting in the military, make certain they do not accept gifts offered by recruiters or share any personal information with them.

SUBMIT A WRITTEN REQUEST to your principal to opt out of providing your high school children's personal information to military recruiters. See Appendix C for a sample form.

ASK YOUR PRINCIPAL how to opt out of "directory information" to prohibit the school from sharing personal information with some third-parties as is your right under the Federal Education Rights and Privacy Act or FERPA. Your school should provide you these

forms without being asked, but many don't. Also, schools often have a deadline to opt out of directory information disclosure, typically within the first ten to thirty days of a school year. For more on this, see Section II and Appendix B for a sample directory information opt out form.

EXERCISE YOUR RIGHTS under FERPA to access and review your children's educational records at the school and district level each year, as well as records contained in the statewide longitudinal data system (SLDS). Ask to correct any mistakes you see in these records. For more information about the SLDS, see Sections II and VII. To request access and review your child's records, use the sample request form in Appendix A.

WHEN REGISTERING YOUR CHILDREN for College Board's PSAT/SAT or ACT exams, do not check the box to opt into sharing extraneous personal information with colleges or other organizations, and do not provide these companies with any unnecessary information. Your children may also be asked to provide personal information again on exam day; they should be discouraged from checking the box or providing anything other than name, grade, school, and other details required to take the test. When students fill in this additional information, the data is often sold by the testing companies to colleges and others, to be used for marketing and recruitment, or to help colleges decide who to accept or reject.

Prior to the test, your child's teacher may read aloud instructions prepared by the College Board/ACT that may make it sound to students as if they are required to answer personal questions. Make sure you inform your child before the test that providing answers to any questions touching on the subjects below is strictly voluntary.

Questions may touch on the following sensitive subjects:
- *contact information;*
- *major;*
- *gender;*
- *disability status;*
- *grades and rank;*
- *ethnicity;*
- *religion;*
- *educational aspirations;*
- *parent income and financial aid;*
- *sports;*
- *college living preferences;*
- *citizenship;*
- *ROTC;*
- *desired college characteristics;*
- *high school courses and activities; and*
- *honors.*

What to look for in terms of service and privacy policies

If the terms of service and/or privacy policies of online programs your children use at home or school include any of the red flags below, consider not using the programs. The language should be reviewed by an attorney or school official to ensure they are not in violation of federal or state laws or district policies.

EXAMPLE: "The Company reserves the right, at its sole discretion, to modify or replace any part of this Privacy Policy."

REASON FOR CONCERN: Companies should not be allowed to change their policies without first notifying and obtaining consent from users. In the case of apps used at schools, unilateral changes made by a company may result in inappropriate or even illegal disclosure or use of student information.

For additional examples, refer to the U.S. Department of Education's Privacy Technical Assistance Center at http://ptac.ed.gov/

EXAMPLE: "By using the Service, you are authorizing the Company to use, gather, parse, and retain any data related to the delivery of the Service."

REASON FOR CONCERN: Companies should be very explicit about what user data they collect, and how it will be used, shared, and deleted. When apps are used in schools, they are generally allowed to use student information for educational purposes only. To use it for any other purpose — commercial or otherwise — may be a violation of federal law, including FERPA and COPPA.

EXAMPLE: "The Company shares your information with third-party business partners for the purpose of providing the Service to you. We may also share certain information such as browser and cookie data and other data relating to your use of our Service with our business partners to deliver information about products or services that may be of interest to you."

REASON FOR CONCERN: Companies should identify by name, address, phone number, and email address any other third parties collecting or maintaining your children's personal information gathered through the app. If not, they may be in violation of COPPA (if your child is under 13 and the website is child-directed) or FERPA. Additionally, companies should not use information collected about children to develop marketing profiles or serve ads to children or their parents.

EXAMPLE: "The Company and its partners and licensors may collect, use, transmit, process and maintain your location data, including but not limited to the geographic location of your device (e.g., latitude and/or longitude) and information related to your account."

REASON FOR CONCERN: Whether the app is used at home or school, companies should not collect children's geographic location data.

EXAMPLE: "No data transmission over the Internet is 100% secure. The Company will strive to protect your personally-identifying information, but we cannot warrant the security of any information you transmit to us and you do so at your own risk."

REASON FOR CONCERN: Companies should always encrypt users' personal data, employ other best practices to secure data, and should not try to exempt themselves from liability if breaches occur.

CommonSense Media advises parents to "look for the 'https' in the URL" and offers other tips to enhance student data privacy and security at https://www.commonsense.org/education/privacy

Their December 2016 survey revealed that 25 percent of education technology websites did not support encryption, and 20 percent did not require an encrypted connection.[12]

EXAMPLE: "The Company may share information that we collect in connection with a corporate transaction, such as the sale of our services, a merger, consolidation, asset sale or in the event of bankruptcy."

REASON FOR CONCERN: While some state privacy laws ban the sale of personal student data, companies may claim exceptions to allow for the sale of the data in case of a merger, bankruptcy or "asset" sale. Others may claim that they while they will not sell the data, they may "license" it for a fee to other companies or organizations. Parents should be wary of such statements in a corporate terms of service or privacy policy.

Disclaimer: While the goal of the Parent Coalition for Student Privacy and the Campaign for a Commercial-Free Childhood is to provide valuable resources to help you protect student privacy, our suggestions should not be used in place of legal advice from an attorney. For questions on how federal, state, and local laws and policies may apply to your situation, you may wish to seek the advice of a licensed attorney by contacting your local bar association's referral service.

Questions? Visit www.studentprivacymatters.org/toolkit for more information, including free webinars on how to use the resources in this toolkit.

REFERENCES

1. http://well.blogs.nytimes.com/2016/03/08/dont-post-about-me-on-social-media-children-say/?_r=0

2. http://www.nominet.uk/wp-content/uploads/2016/09/Nominet-Share-with-Care-2016-Infographic.pdf

3. http://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/

4. https://www.sciencedaily.com/releases/2016/05/160531104423.htm

5. https://www.eff.org/privacybadger

6. https://getadblock.com/

7. https://www.ghostery.com/

8. http://www.computerworld.com/article/2692560/six-browser-plug-ins-that-protect-your-privacy.html

9. http://www.nytimes.com/2016/06/23/technology/personaltech/mark-zuckerberg-covers-his-laptop-camera-you-should-consider-it-too.html?_r=0

10. http://www.siia.net/Press/SIIA-Estimates-838-Billion-Dollars-US-Market-for-PreK-12-Educational-Software-and-Digital-Content

11. http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip

12. https://www.commonsense.org/education/privacy/survey/encryption