



THE FIGHT FOR STUDENT PRIVACY POST -INBLOOM

Parent Coalition for Student Privacy

Leonie Haimson & Rachael Stickland, Co-chairs
Network for Public Education 3rd Annual Conference
April 16, 2016

www.studentprivacymatters.org

Life and death of inBloom Inc. (2013-2014)

- inBloom Inc. launched in February 2013 with more than \$100M in Gates Foundation funds
- Designed to collect personal information of millions of public school students in nine states and districts, including NY, CO, and NC.
- Data to be shared with for-profit data-mining software companies w/out parental knowledge or consent.
- Data to include student names, addresses, grades, test scores, grades, economic and racial status, disciplinary records, disability information and much else.
- All legal liability assigned to states and districts and starting in 2015, inBloom would start charging for its services.
- Without any funding or institutional backing, parent activists across the country protested and in April 2014, inBloom closed its doors.

With inBloom defeated, what did we learn?

- Parents (and many others) had incorrectly believed federal law protected students' personal identifiable information (PII) in school records by requiring parental notification & consent before disclosure to 3rd parties.
- We were wrong! We learned how FERPA had been weakened in many ways, enabling the sharing of personal data with organizations and companies for many reasons without parents' knowledge
- We also became fully aware for 1st time how much collection and sharing of student data was already occurring by schools and districts with vendors and other 3rd parties.

The inBloom controversy kick-started a huge debate on student privacy that continues:

- 21 states passed 24 new student privacy laws in 2014
- 15 states passed 28 new student privacy laws in 2015
- 5 student privacy bills have been introduced in Congress
- A voluntary student privacy pledge created by the software industry group signed by 220 tech companies.
- ***Yet none of these measures are strong enough.***

Launch of Parent Coalition for Student Privacy

- In summer 2014, we formed a national organization with some of our allies in the inBloom fight
- We are working to inform parents about the myriad threats to student privacy
- We are providing them with suggestions for actions they can take to help strengthen student privacy at the school, district and state levels.

We advocate for stronger federal privacy protections for student data

F:\AS\114\FERP\FAFERPA_002.XML

(Original Signature of Member)

114TH CONGRESS
1ST SESSION

H. R. _____

To amend the General Education Provisions Act to strengthen privacy protections for students and parents.

IN THE HOUSE OF REPRESENTATIVES

Mr. BOKUNIA (for himself, Ms. FUDGE, Mr. KLINE, and Mr. SCOTT of Virginia) introduced the following bill; which was referred to the Committee on

A BILL

To amend the General Education Provisions Act to strengthen privacy protections for students and parents.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*
3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the "Student Privacy Pro-
5 tection Act".

6 **SEC. 2. REFERENCES.**

7 Except as otherwise expressly provided, whenever in
8 this Act an amendment or repeal is expressed in terms

Testify before Congress on the need to require more transparency around disclosure and security protections for student data



U.S. House Committee on Education and the Workforce, March 22, 2016.

Speak at state and district forums

THE STUDENT DATA MINEFIELD Informational Forum on Student Data Privacy

Thursday, January 21, 2016
12:00-2:00pm
Legislative Office Building, Hartford, CT
Room 1E

Google Under Fire for Data-Mining Student Email Messages
Education Week

Nevada Dad Told It Will Cost \$10K to See School Data School Collected on His Children
Nevada Journal

Millions of Student Records Sold in Bankruptcy Case
Education Week

Dispute Erupts Over Release of Data on Hamden School Students
Hartford Courant

Privacy Fear Over Student Data Tracking Lead to iBloom's Shutdown
Bloomberg Business

The explosion in student data mining beyond the classroom poses great risk to the safety, privacy, and civil liberties of children and families.

WHO is collecting teacher and student data? WHO can get it? WHAT are the risks? WHAT has changed? WHAT is FERPA? HOW have other states acted to increase data protections? WHAT can parents, legislators, educators, and local communities do?

MODERATOR
Rep. Andrew Fasichmann, Co-Chair, Education Committee

SPEAKERS

- Khaleh Barnes, Electronic Privacy Information Center (EPIC), Washington, D.C.
- Cameron Russell, Executive Director, Center on Law and Information Policy (CLIP) at Fordham University School of Law.
- Leonie Haimson, co-chair, Parent Coalition for Student Privacy
- Brian Kelly, Chief Information Security Officer, Quinnipiac University

REGISTER by going to www.regonline.com/studentdataminefield. Help us plan this event by sharing your insight.

CEA
Advocating for students and teachers

Connecticut Education Association Informational Forum on Student Privacy & Data Mining


Recorded On: 1/21/2016

LEONIE HAIMSON
Founder & Co-chair
Parent Coalition for Student Privacy

CTN
01/21/16

1:37:44 1:55:45 CC

Provide fact sheets on student privacy rights under existing federal law



Parent Coalition for Student Privacy

ABOUT US JOIN US BLOG **PRIVACY RESOURCES** LEGISLATION INBLOOM ACTION MEDIA PRIVACY POLICY

Follow me

My Page Use

FEDERAL STUDENT PRIVACY RIGHTS: FERPA, PPRA AND COPPA

[Your Rights under FERPA](#)

[Your Rights under PPRA](#)

[Your Rights under COPPA](#)

FERPA

The Family Educational Rights and Privacy Act ([FERPA](#)) (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law passed in 1974 that bars the disclosure of personally identifiable data in student records to third parties without parental consent. Yet FERPA has been considerably weakened in recent years to make it possible to enable schools and districts to share these data with others for a multitude of reasons, including allowing it to be disclosed to vendors, consultants and contractors for administrative, instructional or assessment purposes (known as the "school official/contractor" exception) and/or to organizations or individuals for vaguely-defined evaluation or audit purposes, without either notifying parents or gaining their consent (known as the "authorized representative" exception). In addition, yet a third loophole allows nonconsensual disclosures (and re-dis-

DONATE TO PROTECT STUDENT PRIVACY

Amount: \$ [DONATE NOW](#)

JOIN OUR COALITION

RECENT POSTS

Parent attacked by iNACOL and her son's data disclosed for questioning "blended" learning
April 11, 2016
Heather Hicks is a parent and teacher who resides in Lacey Township, New Jersey. She spoke up at her school board meeting, criticizing Edgenuity - an online learning program produced by Pearson that her son's school was using. In Heather's ... [Read More](#)

Send a Letter to the Education Commissioners in the PARCC and SBAC states
April 5, 2016
The letter from Parent Coalition for Student Privacy, Parents Across America, Network for Public Education, FairTest and many state and local parent groups to the Education Commissioners in the PARCC and SBAC states on the machine scoring of their Common Core exams ... [Read More](#)

Rachael Stickland testifies to U.S. House Education & the Workforce Committee on Student Privacy
March 28, 2016
On Tuesday, March 22, 2016, Parent Coalition for Student Privacy co-chair Rachael Stickland was invited to testify

Help parents write FERPA complaints when their schools violate those rights

NYC Public School Parents

Independent voices of New York City public school parents

Thursday, October 22, 2015

Cease and Desist letter sent today to Eva Moskowitz of Success Charters

A FERPA complaint to the US Dept of Education Family Compliance Office will follow soon.

Cc: john.merrow@gmail.com

Viewermail@newshour.org

mgetler@pbs.org

Ann.Powell@successacademies.org

October 22, 2015

Eva Moskowitz, CEO

Success Academy Network

95 Pine Street, Floor 6, New York, NY 10005

By US Postal Service Priority Mail and email to: eva.moskowitz@successacademies.org

Dear Ms. Moskowitz;

I demand that you immediately remove the letter you wrote to PBS and sent to the press on October 19, that contained details of my son's disciplinary record and is posted at [link removed] , as well as the second follow up letter you posted and sent on October 21 at [link removed.]

As you are well aware, regulations governing compliance with the Family Educational Rights and Privacy Act of 1974 require that educational agencies and institutions obtain a parent's signed and dated written consent before they are allowed to share non-directory personally identifiable information from a student's education records to third parties (34 CFE 99.30).

Raise awareness through articles and opeds


The Washington Post

Answer Sheet

What your child needs to know before taking the SAT and ACT

A 1 Save for Later Reading List

By Valerie Strauss January 21 Follow @valeriestrauss



(Bigstock)

Millions of students will take the ACT and SAT this year (including this Saturday, the date of the last administration of the SAT that is being retired in favor of a new version), and students may be surprised to find non-academic queries that they aren't expecting to answer. The College Board, which owns the SAT, and ACT pose non-academic questions for students willing to

Most Read

- 1 Teacher: What third-graders are being asked to do on 2016 Common Core test
- 2 The ugly truth about Confederate memorials
- 3 This white nationalist who shoved a Trump protester may be the next David Duke
- 4 White House intervenes in Maryland Senate Democratic primary
- 5 Obama to forgive the student debt of permanently disabled people

Our Online Games

Play right from this page

Mahjongg Dimensions
Genre(s): Strategy
It's 3D Mahjongg you don't even need to wear 3D glasses!

The Sunday Crossword by Evan Birnholz
Genre(s): Word
Online crossword.


The Washington Post

Answer Sheet

The astonishing amount of data being collected about your children

A 21 Save for Later Reading List

By Valerie Strauss November 12, 2015 Follow @valeriestrauss



Big data is no longer a tool reserved solely for big businesses. (Alan Brandt/AP)

Parental concerns about student privacy have been rising in recent years amid the growing use by schools, school districts and states use technology to collect mountains of detailed information on students. Last year, a controversial \$400 million student data collection project funded by the Gates Foundation and operated by a specially created nonprofit organization called inBloom was forced to shut down because of these concerns, an episode that served as a warning to parents about just how much information about their children is being shared without their knowledge.

Most Read

- 1 Teacher: What third-graders are being asked to do on 2016 Common Core test
- 2 The ugly truth about Confederate memorials
- 3 This white nationalist who shoved a Trump protester may be the next David Duke
- 4 White House intervenes in Maryland Senate Democratic primary
- 5 Obama to forgive the student debt of permanently disabled people

Our Online Games

Play right from this page

Mahjongg Dimensions
Genre(s): Strategy
It's 3D Mahjongg you don't even need to wear 3D glasses!

The Sunday Crossword by Evan Birnholz
Genre(s): Word
Online crossword.

Alert parents on how to comment on proposals to expand federal collection of student data

System of Records--Impact Evaluation of Data-Driven Instruction Professional Development for Teachers

Docket Browser [Return to Docket Folder Summary](#)

Docket ID: ED-2015-IES-0100 Agency: Department of Education (ED)

New Search within this Docket Search Within Results

[Export](#) | [Sign-up for Email alert](#)

Filter Results By...

Document Type i

Clear Filter

- Notice (2)
- Proposed Rule (0)
- Rule (0)
- Supporting & Related Material (0)
- Other (0)
- Public Submission (182)

Posted i

Search All

Comments Due i

Search All

184 results

Results per page: 25

Sort By: Best Match

Comment on FR Doc # N/A

No! You do not have rights to my children's personal information.

Public Submission | Posted: 02/25/2016 | ID: ED-2015-IES-0100-0164

Submitter Name: Jessica Garcia

Comment Period Closed

Feb 18, 2016 11:59 PM ET

Comment on FR Doc # N/A

No identifiable information should be collected without PARENTENTAL consent. Parents should have the final say in any and all matters having to do with their children.

Public Submission | Posted: 02/25/2016 | ID: ED-2015-IES-0100-0150

Submitter Name: Anonymous Anonymous

Comment Period Closed

Feb 18, 2016 11:59 PM ET

Comment on FR Doc # N/A

I am the mother of a 2nd grader and a 3 year old. I am also the wife of a federal employee in which his OPM file was Breached as well as our entire family being victim of insurance...

Comment Period Closed

Inform parents about risks to privacy of state data collection & sharing

- 2009, US Dept. of Education required states to develop state longitudinal data systems (SLDS) in which personal student data is combined with health and medical information, juvenile justice, Child services – to track children “cradle to the grave.”
- US ED also helping to develop Common Education Data Standards, now with more than 1500 data pts including health data, early child development info, disciplinary infractions, disabilities, socio-emotional skills, health information, detailed family information & assessment/achievement results.
- We are advocating for creation of Stakeholder Data Advisory boards at the state level--- to involve parent in the decision making of what data to collect and how to restrict further disclosures.

Most recently, we drafted a letter to PARCC/SBAC states asking whether they're using computer scoring

SEND A LETTER TO THE EDUCATION COMMISSIONERS IN THE PARCC AND SBAC STATES

🕒 APRIL 5, 2016 ✎ EDIT

The letter from Parent Coalition for Student Privacy, Parents Across America, Network for Public Education, FairTest and many state and local parent groups to the Education Commissioners in the PARCC and SBAC states on the machine scoring of their Common Core exams this spring is below. Please send your own letter to your State Chief if you are in one of these states. More information about the lack of evidence for machine scoring is in this [issue brief here](#).

UPDATE: In response to our (or reporter) queries, PARCC finally posted their study from March 2014 on automated efficacy [here](#). The SBAC au-

We developed five privacy principles that every school and district should uphold

- Increased transparency on disclosure and use of student data
- No commercial uses of personal student information
- Strong data security measures to protect against breaches
- Robust enforcement of laws and best practices
- Maximize parental and student rights for notification and consent

Transparency and no commercial uses

- **1. Transparency:** Parents must be notified by their children's school or district in advance of any disclosure of personally identifiable info to any third parties outside of the school or district.
 - All disclosures should require publicly available contracts and privacy policies that specify which data are disclosed for what purposes, and provide a date certain when the data will be destroyed.
- **2. No commercial uses:** Selling of personal student data and; or use for marketing purposes should be banned. ***NO advertising should be allowed on instructional software or websites*** assigned to students by their schools, since ads are a distraction from learning and serve no legitimate educational purpose.
 - While some of the current federal and state bills ban "targeted" ads, others ban targeted ads except for those derived from a student's one-time internet use. But how can any parent know whether an ad displayed to their children was based on data-mining, either a single time or over a longer period?

Security and enforcement

- **3. Security protections:** At minimum, encryption of personal data at motion and at rest should be required
 - Training for all individuals with access to personal student data, audit logs, and security audits by an independent auditor.
 - Passwords should be protected in the same manner as all other personal student information.
 - There must be notification to parents of all breaches, and indemnification of the same.
 - No “anonymized” or “de-identified” student information should be disclosed without verifiable safeguards to ensure data cannot be easily re-identified.
- **4. Enforcement:** The law should specify fines if the school, district or third party violates the law, their contracts and/or privacy policies; with parents able to sue on behalf of their children’s rights as well.
 - Without strong enforcement provisions, any law or policy protecting student privacy is likely to be ignored.

Parental and student rights

- **5. Parental/Student rights:** NO re-disclosures by vendors or any other third parties to individuals, sub-contractors, or organizations should be allowed without parental notification and consent (or students, if they are 18 or older).
 - Parents must be allowed to see any data collected directly from their child by a school or a vendor delete the data if it is in error or is nonessential to the child's transcript, and opt out of further collection.
 - Any data-mining for purpose of creating student profiles, even for educational purposes, must be done with full parental knowledge.
 - Parental consent must be required for disclosure of personal data, especially for highly sensitive information such as their child's disabilities, health and disciplinary information.

Write privacy toolkits

We're partnering with the Campaign for a Commercial-Free Childhood to develop privacy toolkits for parents and teachers.



Campaign for a Commercial-Free Childhood



What will the toolkits contain?

- **Practical guidance** for parents and teachers to protect their students' privacy and data security.
- **Best practices** for parents and teachers to protect their students' privacy and data security.
- **Tools for parents (and teachers) to advocate** for stronger privacy and data security protections at the school and district.

What will the toolkits contain?

Practical guidance, including:

- At the beginning of the school year, opt-out of directory information which will prohibit the school from sharing personal information with some third-parties including military recruiters.
- Do not opt-in to sharing personal information with scholarship providers and universities when your child takes the SAT or ACT exams.
- Teach your child how to create accounts without using student name/student number, and how to select a secure password that doesn't disclose personal information about a child (i.e. pet's name).

What will the toolkits contain?

Best practices, including:

- Schools/Districts should tell parents about what personally identifiable information they are collecting on students and how it's being used and protected from breaches
- For sensitive information, parental consent should be obtained before a child's personal information is shared with third parties
- States and districts should develop a process to vet and approve classroom apps and online programs to ensure they comply with the law and best privacy and security practices.
- Teachers should be prohibited from using apps and online programs that have not been properly vetted or approved by the state or district.

What will the toolkits contain?

Advocacy tools, including:

- Conversation guide or “primer” to help parents open the dialogue with their teacher/principal/school board; may include sample letters.
- Tips for parents to approach district administration or the school board to advocate for stronger student privacy policies.

Will you help us?

Stakeholder interviews; general feedback:

The toolkits should support relationship building:

- **Parents** are most comfortable coming from a place of curiosity, using “soft words” and asking questions.
 - "I'm curious about information stored in the cloud, can you help me understand...?"
 - “Can you help me understand the privacy policy of the apps my child is using?”
- Toolkit resources should empower **teachers**.
 - “You are the first line of defense...” and “without laws, you can make choices/decisions that make sense...” and “you can make an impact now.”
 - Can use analogies that resonate, i.e. “You would discourage your student from sharing personal information broadly on the Internet or with a stranger on the street, maybe that information shouldn’t be shared with an app, etc.”

Stakeholder interviews; common themes:

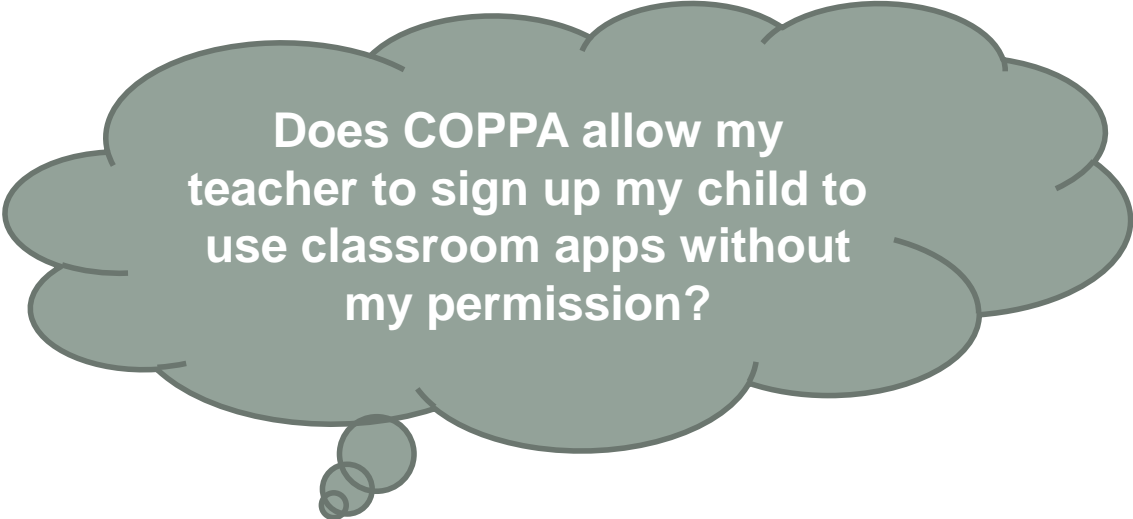
Parents and teachers have very little understanding about the issues and concerns with privacy and data security in schools:



Stakeholder interviews; common themes:

Parents need to know their rights and teachers need to know their responsibilities under existing law:

- Federal laws – FERPA, COPPA, PPRA
- State laws – ever-changing landscape
- How do local school district policies interact?



Does COPPA allow my teacher to sign up my child to use classroom apps without my permission?

Stakeholder interviews; common themes:

Parents want to know “practical guidance” they **can use at school and at home** to keep their children’s information private and safe, especially when using school-issued devices or online programs/apps.

- At the beginning of the school year, opt-out of directory information which will prohibit the school from sharing personal information with some third-parties including military recruiters.
- Do not opt-in to sharing personal information with scholarship providers and universities when your child takes the SAT or ACT exams.
- Teach your child how to create accounts without using student name/student number, and how to select a secure password that doesn't disclose personal information about a child (i.e. pet's name).



Opt out of directory information

Stakeholder interviews; common themes:

Parents want to know “best practices” they **can suggest to schools and districts** to keep their children’s information protected.

- Schools/Districts should tell parents about what personally identifiable information they are collecting on students and how it's being used and protected from breaches.
- For sensitive information, parental consent should be obtained before a child’s personal information is shared with third parties.
- States/districts should develop a process to vet and approve classroom apps and online programs to ensure they comply with the law and best privacy and security practices.
- Teachers should be prohibited from using apps and online programs that have not been properly vetted or approved by the state or district.



without permission!

Stakeholder interviews; common themes:

Parents **need tools to help advocate** for “best practices” and stronger district policies governing student privacy.

- Conversation guides or primers parents can use to open the dialogue, including sample letters to teachers/principals/boards of education.
- Building a coalition of support to approach school or district administration.
- Organizing community meetings to affect policy change at the district or state level.



Questions:

- Are there any **existing resources** we should know about?
- Is there any specific advice we should include regarding **practical guidance**?
- Is there anything specific we should include regarding **best practice**?
- What **tools do you need to advocate** for best practices and improved privacy policies and procedures?

For more information...

- We have fact sheets on parental rights under FERPA, COPPA, and PPRA as well as opt out forms available at www.studentprivacymatters.org
- You can also ask us questions at info@studentprivacymatters.org
- Sign up for our newsletter for updates at our website at www.studentprivacymatters.org
- Join our Facebook page and follow us on Twitter [@parents4privacy](https://www.facebook.com/parents4privacy)

Parental rights under FERPA

- Right for your child's educational records NOT to be disclosed publicly (except for operational, educational, research, or evaluation exceptions.)
- Right to inspect the information in your child's education records, held by school, district or state & correct data if it's erroneous – including in the SLDS.
- Right to be informed of school/district's criteria to determine who constitutes a “school official” with whom PII can be shared without parental consent.
- Right to opt out of the child's “directory information” being shared—including name, address, email, telephone number, date & place of birth etc. –as long as the school/district has no agreement with the vendor to share data for exceptions noted above.
- Right to opt out of having their child's name, address and telephone provided to military recruiters.
- Right to be informed of their FERPA rights each year by their school or district.

Parental rights under Children's Online Privacy Protection Act (COPPA)

- If your child participates in online services at home or school, COPPA applies, regulated by FTC.
- Your school should be providing you with a list of all the online programs that your child participates that gains access your child's personal information, according to FTC "best practice."
- If your child is under-13 the school and/or vendor or operator must provide the school with a clear and prominent privacy policy, including the following information:
 - The name, address, telephone number, and email address of the vendors collecting or maintaining personal information through the site or service;
 - The types of personal information the operator is collecting, how the data is being used and with whom it may be shared;
 - That the school can request to review or have deleted the child's personal information;
 - That the school can refuse to permit its further collection or use..

Parental rights under the Protection of Pupil Rights Amendment (PPRA)

- **1.** Right of parental consent before child is required to participate in federally funded survey, analysis or evaluation dealing with information concerning:
 - Political affiliations; mental or psychological problems; religious affiliations and beliefs;
 - Sexual behavior and attitudes; illegal anti-social, self-incriminating or demeaning behavior;
 - Critical appraisals of individuals with whom respondents have close family relationships;
 - Privileged relationships, with lawyers, physicians, and ministers;
 - Income (other than that required by law to determine eligibility for a program).
- **2.** If the survey or evaluation is not federally funded, written consent not required but parents must be notified in advance & have the right to opt their children out.
- **3.** In either case, schools and/or their contractors must make these materials or surveys available for inspection by parents ahead of time.