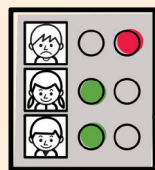# SECTION I.
What is student data?

To fully understand the types and amount of personal information a student generates in today's digital world, and how it's used and shared, let's examine the life of a fictitious child named Tommy and his journey through a data- and technology-driven school experience.
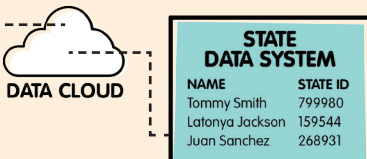
1. Before he starts kindergarten, Tommy's parents must provide his school with his personal information including name; gender; date of birth; social security number; health information (e.g., immunizations, prescribed medications, disabilities, allergies, etc.); and family income information to see if he qualifies for free or reduced-priced lunch.
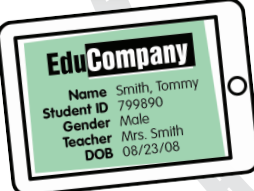
Tommy's information is then uploaded into the district's online database — which is likely maintained by an out-of-state company such as InfiniteCampus and stores all data in the "cloud" — and provided to school administrators, teachers, and parents via a digital "data dashboard."

The school will send much of the information electronically to the state department of education to track Tommy's progress through school in the statewide longitudinal data system (SLDS). Researchers and policymakers often use this information for accountability and evaluation purposes.

2. Before Tommy arrives in the classroom for his first day, his personal information is shared with various companies that provide services to the school and district. The district creates Tommy's school bus and online lunch account and ID card, and signs him up with Google's G Suite for Education.

3. On his way to school, Tommy's location and internet activity are tracked by technology installed on his school bus.

A radio frequency identification (RFID) chip in Tommy's ID card allows the school to track his whereabouts.

If Tommy allows his smartphone or tablet to connect to the Wi-Fi while riding on the bus, his login and browsing information may be tracked by the internet provider and school district.

4. While in class, if Tommy speaks without raising his hand, his teacher records the event in his Class Dojo account — an online behavior management tool. The system emits an audible "BONG" for the entire class to hear and adds a demerit to his online profile. Daily and weekly updates are sent to Tommy's parents via a phone app, text, or email.

5. In the cafeteria, Tommy provides his fingerprint, name, or student number to the lunchroom aide, who then records his food selections in his online account, which may become a part of his permanent digital record.

6. During gym class, Tommy wears a heart rate monitor to record his workout intensity as part of his grade. An app analyzes the results and sends a report via email to the teacher's Dropbox account. It's unclear what happens to Tommy's digital health information at the end of the school year.
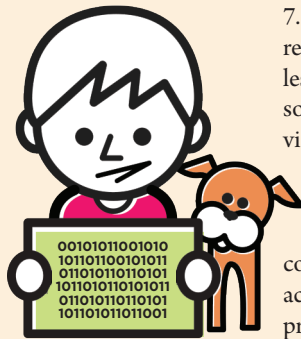
7. At home and school, Tommy receives "personalized learning" lessons online. Whether he's solving math problems via a video game or taking quizzes after reading a story, for-profit technology companies — *not* his teachers — determine the content and difficulty level of the activity by collecting data and using proprietary algorithms to analyze his abilities, profile his interests, and predict outcomes. This process is known as "data mining."

8. Starting as early as Kindergarten, Tommy is assigned interim assessments or test prep to meet district and state requirements. In grades 3 through 8, he takes annual standardized exams in math and English Language Arts (ELA) as required by federal law. He may also be subjected to various local and periodic standardized assessments in these and other subjects. Companies administering these tests often collect an array of sensitive personal information from students, as well as metadata like the amount of time they spend answering a specific question. Essays are often scored by machines rather than people.

9. Sometime during elementary school, Tommy may be asked to complete "school climate" and other surveys measuring his personal beliefs, his political views, or social and emotional skills, often using an online account with his name or other personal information attached to it.

10. As Tommy progresses through his elementary and middle school years, his education record grows to include grades, course schedules, standardized test scores, disciplinary information, counseling records, disabilities and 504 or Individualized Education Plans, and any health condition he might have that requires medication or special treatment in school. The file may also include information on his family history, his racial and ethnic background, his country of birth, whether he is an immigrant or homeless, and what special services he receives.
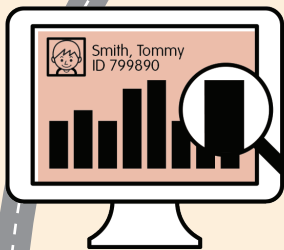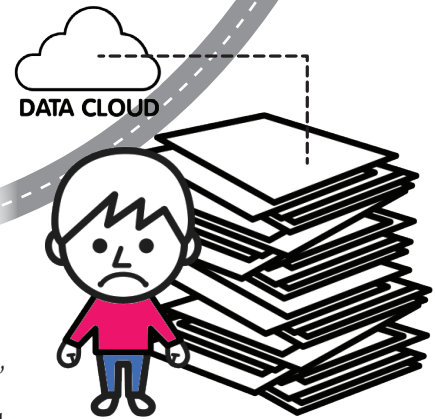
11. When Tommy reaches sixth grade or even sooner, his district may implement a 1:1 program. District-provided devices will be issued to each student with default settings that allow companies like Google to track and mine student data, including internet sites visited and search terms used, books and articles read online, videos watched on YouTube, and passwords. Tommy uses this device until he graduates, amassing millions of data points that can be mined to diagnose his learning issues, steer him towards certain courses or careers, or generate a consumer profile that can be sold by data brokers.
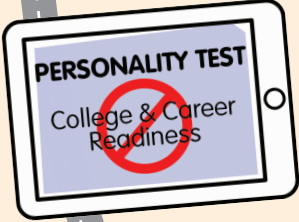
12. Without the knowledge or consent of his parents, Tommy's school district may share his name, course grades, attendance records, disciplinary records, standardized test scores, and disabilities with private researchers and even the U.S. Department of Education. Study results will never be provided to Tommy or his family.

WHAT ARE THE FACTS ABOUT "PERSONALIZED LEARNING" PRODUCTS? According to a 2016 paper by the Data & Society Research Institute, "Most product websites describe the input of teachers or learning scientists into development as minimal and after the fact (Guernsey & Levine, 2015). Products are not field tested before adoption in schools and offer limited to no research on the efficacy of personalized learning systems beyond testimonials and anecdote."[1]

HOW DO PARENTS FEEL ABOUT STUDENT PRIVACY? A 2015 study by the Future of Privacy Forum found that 87% of parents surveyed "worry about student data being hacked or stolen." The study also found that 68% of parents surveyed are concerned "that an electronic record would be used in the future against their child by a college or an employer."[2]
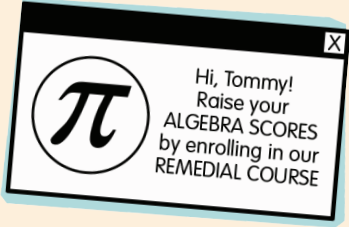
WHAT HAPPENS TO DATA CAPTURED ONLINE? When students browse the internet − whether at home or school − their information is collected by online companies, bundled as consumer profiles, and then sold in the shadowy data market. Because this data has the potential to accurately predict feelings, motivations, and behaviors, it may be purchased by colleges, employers, mortgage lenders and insurance underwriters to evaluate an individual's suitability for those services and products.

13. By the time Tommy is in middle school, he is encouraged or required to use an online program like Naviance to complete surveys and set personal and academic goals to plan for college. Once in high school, he will be required to use much of the information stored in Naviance to apply for college.

14. In high school, Tommy registers for an online course or instructional app in addition to his traditional classes. Some online courses, like those offered by a company called Knewton, collect millions of data points on each student per day. Information Tommy provides online companies may be used to advertise products or programs to him or his parents, based on his personal data.

Hi, Tommy! Raise your ALGEBRA SCORES by enrolling in our REMEDIAL COURSE

15. In high school, Tommy takes College Board Advanced Placement (AP) courses and exams, the PSAT, SAT, and/or the ACT, before which he will be asked a series of personal questions. The College Board or ACT may then sell his student profile to colleges to help them decide whether to recruit and admit him or not, if he unknowingly gives his consent.

Smith, Tommy
ID 799890
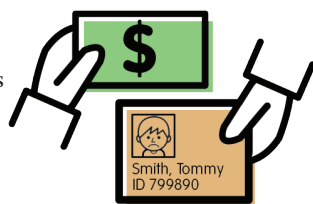
16. When Tommy is a sophomore or junior, his private information may be shared with military recruiters unless his parents revoke their permission in writing. Regardless, his school may administer the Armed Services Vocational Aptitude Battery (ASVAB) exam and release his results to recruiters.

K-12 DATA
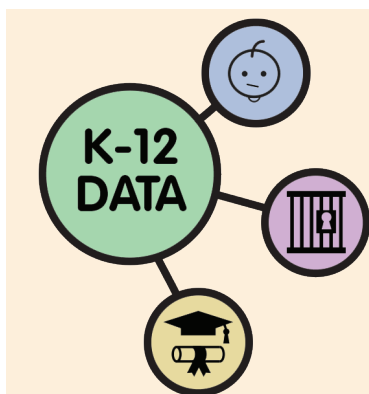
18. By the time Tommy graduates, his education record spans more than 13 years. Each year of school, his district sent much of the information in his record to the statewide longitudinal data system (SLDS) where it may be linked to other state agency databases, including the departments of health and human services, higher education, and corrections, and then passed along to researchers.

At any point in Tommy's educational career, his personal data, whether held by his school, state or federal agencies, researchers, or online vendors, may have been misused, breached, or hacked, damaging his future prospects in ways beyond our current imagination.
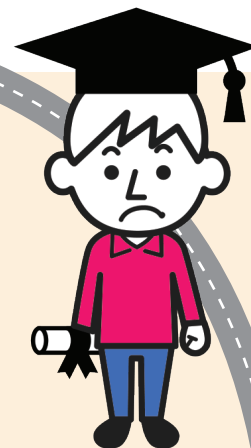
HAS STUDENT DATA STORED IN STATE SYSTEMS OR SLDS BEEN MISUSED? In March 2016, a judge ordered the records of 10 million California students, including "names, addresses, disciplinary records, grades, test scores, and even details such as pregnancy, addiction and criminal history," to be made available to a private organization suing the state for access to the student database.[3]

HAS STUDENT DATA BEEN BREACHED BY SCHOOLS? In February 2016, Washington D.C. Public Schools publicly posted the private information of approximately 12,000 public school special needs students online, including "each student's identification number, race, age, school, disabilities and any services he or she receives."[4]

DO COMPANIES OFFERING ONLINE "LEARNING" PRODUCTS GET HACKED? In late 2015, VTech, an "award winning electronic learning toy company," had 4.9 million parent accounts and 6.4 children profiles breached by a hacker. Parent information included "name, mailing address, email address, IP address, download history and account credentials." Child profiles included name, gender, and birthdate.[5]

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

REFERENCES

1. https://datasociety.net/pubs/ecl/PersonalizedLearning_primer_2016.pdf

2. https://fpf.org/wp-content/uploads/2015/11/Beyond-the-Fear-Factor_Sept2015.pdf

3. http://www.mercurynews.com/bay-area-news/ci_29590794/judge-pulls-back-from-calif-student-records-release

4. https://www.washingtonpost.com/local/education/dc-accidentally-uploads-private-information-of-12000-students/2016/02/11/7618c698-d0ff-11e5-abc9-ea152f0b9561_story.html

5. https://www.washingtonpost.com/news/the-switch/wp/2015/12/01/vtech-says-6-4-million-children-were-caught-up-in-its-data-breach/