



January 2020

Office of the General Counsel

Privacy

Sarah McGee

Assistant General Counsel



**What is
Privacy?**

The Right to Privacy

- “The right to be left alone”
 - Samuel Warren & Louis Brandeis, 1890 Harvard Law Review
- “The state or condition of being free from being observed or disturbed by other people.”
 - Oxford Dictionary
- “Having control over how information flows”
 - danah boyd, "Making Sense of Privacy and Publicity". SXSW, March 13, 2010
- “The right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used.”
 - IAPP
- Privacy consists of (1) an individual’s ability to conduct activities without concern of or actual observation and (2) the appropriate protection, use, and release of information about individuals.
 - University of California Statement of Privacy Values

Why is Privacy Important

- Autonomy and individuality – control over our own lives
- If you lived your life under observation, what would change?
 - Less likely to try new things?
 - More afraid to act politically?
- Privacy is a limit on power (both by government and private companies)
- Academic and intellectual freedoms – the ability to speak and research without intimidation – are at the heart of our mission.

What's the Difference Between Privacy and Security?

Privacy

The rights you have to control your personal information and how its used.

Security

How your personal information is protected from breach or exploitation.

Security is necessary, but not sufficient for addressing privacy

Sale or sharing of your personal information might be a privacy violation, but not a security violation.

How Do You Increase Your Privacy?

Online:

- Turn off tracking
- Disable location services, WIFI and Bluetooth
- Choose vendors carefully
- VPN (maybe)
- Fictitious names and dates
- End-to-end encryption
- Strip photos of EXIF data
- Opt out of interest-based tracking

Offline:

- Post office box or commercial mail receiving agency
- Unlisted phone number
- Tinted windows
- Refuse discount / loyalty cards
- Shredding documents
- Pay in cash or cryptocurrency

Right to Privacy – Legal Basis

- The legal sources of privacy law come from a variety of places:
 - U.S. Constitution
 - Tort & contract case law
 - Federal and state laws and regulations
 - Foreign laws (e.g., GDPR)
- No single federal law regulating privacy and the collection, use, disclosure and security of personally identifiable information.

Right to Privacy – Constitutional Basis

“Reasonable expectation of privacy” *implied* in various amendments to the U.S. Constitution

- 1st Amendment – freedom of speech and freedom of assembly (protects the privacy of beliefs)
- 3rd Amendment – protects the privacy of the home (from housing soldiers)
- 4th Amendment – protects from unreasonable government searches and seizures (including computer and mobile devices)
- 5th Amendment – protects against self-incrimination (the privacy of personal information)
- 9th Amendment – “enumeration in the Constitution of certain rights shall not be construed to deny or disparage other rights retained by the people”
- 14th Amendment (Due Process Clause) – “No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protections of the law.”
- The US Supreme Court in *Griswold v. Connecticut* found that taking the above together the Constitution creates a “zone of privacy”

Right to Privacy – State Law Basis

- State Constitutions
 - Article 1, Section 22 of the Alaskan Constitution states “the right of the people to privacy is recognized and shall not be infringed.”
 - Article 1, 1 of the Californian Constitution “articulates privacy as an inalienable act.”
 - Article 1, § 23 of the Floridian Constitution states “every natural person has the right to be let alone and free from governmental intrusion into the person’s private life except as otherwise provided herein.”
 - Article 2, § 10 of the Montanan Constitution states “the right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.”
 - Article 1, § 7 of the Washington Constitution states “no person shall be disturbed in his private affairs, or his home invaded, without authority of the law.”
 - Not in Minnesota’s
- State Laws
 - California – CCPA – January 1, 2020
 - Nevada – October 1, 2019 – ability to opt out of sale of personal information
 - Maine – July 2020 – requires ISPs get approval before customer information is shared / sold to any third parties.

Right to Privacy – Minnesota State Law Basis

- Minnesota Government Data Practices Act
 - Protects private data in the hands of state agencies and municipalities and notification of any breach. Minn. Stat. § 13.055
 - Requires Tennessee notice upon collection of private data for how it will be used and whether you can refuse to provide it. Minn. Stat. § 13.04, subdivision 2.
 - Requires a privacy policy:
 - A government entity that creates, collects, or maintains electronic access data or uses its computer to install a cookie on a person's computer must inform persons gaining access to the entity's computer of the creation, collection, or maintenance of electronic access data or the entity's use of cookies before requiring the person to provide any data about the person to the government entity. As part of that notice, the government entity must inform the person how the data will be used and disseminated, including the uses and disseminations in subdivision 4.
 - Website must remain functional if a user refuses cookies.
 - Minn. Stat. §13.15

Right to Privacy – Minnesota State Law Basis

- Data Breach Statute for private entities – Minn. Stat. 325E.61
 - Any person or business that conducts business in this state, and that owns or licenses data that includes **personal information**, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
 - “personal information” means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:
 - (1) Social Security number;
 - (2) driver's license number or Minnesota identification card number; or
 - (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Right to Privacy – Minnesota State Law Basis

- Minn. Stat. § 325M.02
 - Prohibits ISPs from disclosing personally identifiable information concerning a consumer of the ISP.
- The Minnesota Privacy of Communications Act, Minn. Stat. § 626A.01 – nearly identical to the Federal Wiretapping Act
 - makes it generally unlawful for any person to intentionally intercept, record, disclose or use any oral or wire communications made by persons who would have an expectation of privacy reasonably justified by the surrounding circumstances.

Right to Privacy – Minnesota State Law Basis

- Genetic Testing
- Access to Employee Personnel Records
- Use of SSNs
- Access to Employee Assistance Programs
- Privacy of Nursing Mothers
- No reprisal for employee's political activities or charitable donations

Right to Privacy – Case Law Basis

- Tort Law – “Invasion of Privacy”
 - Intrusion Upon Seclusion
 - Public Disclosure of Private Facts
 - Appropriation of Name or Likeness
 - False Light
- First three torts recognized in 1998
- Contract Law
 - NDAs

Right to Privacy – Other Laws

- Health Insurance Portability and Accountability Act (HIPAA) – enforced by DHS Office of Civil Rights
- Family Educational Rights and Privacy Act (FERPA) – enforced by FPCO
- Federal Trade Commission Act (FTC)
- Telephone Consumer Protection Act (Do Not Call List) (TCPA) – enforced by FCC
- Electronic Communications Privacy Act (ECPA)
- Computer Fraud & Abuse Act (CFAA)
- Children’s Online Privacy Protection Act (COPPA)
- Video Privacy Protection Act (VPPA) – private right of action
- Driver’s Privacy Protection Act (DPPA) - private right of action
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)
- Financial Services Modernization Act (aka GLBA)
- Fair Credit Reporting Act (FCRA) – enforced by FTC & CFPB
- Fair and Accurate Credit Transactions Act (FACTA)
- EU General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)



Right to Privacy – Attempt at State Legislation

- Personal Rights in Names Can Endure Act
 - Proposed by the Minnesota Legislature 2016
 - To codify the right of publicity
 - “an individual has a property right in the use of that individual’s name, voice, signature, photograph, and likeness in any medium in any manner.”
 - Makes it a violation to use a name, voice, signature, photograph, or likeness without consent
 - On Products/Merchandise
 - For Advertising/Selling Goods
 - For Fundraising/Soliciting Donations

Right to Privacy – Attempt at State Legislation

- Personal Rights in Names Can Endure Act
- The PRINCE Act was withdrawn
 - Didn't set a maximum term – allowed an estate to control the right forever (until abandoned), including post copyright. (e.g., a Prince dance party in 2086)
 - Anything that “evokes” a person's identity was too broad
 - Allowed more than damages – allowed court order to take content off line and attorneys fees

Future State Legislation

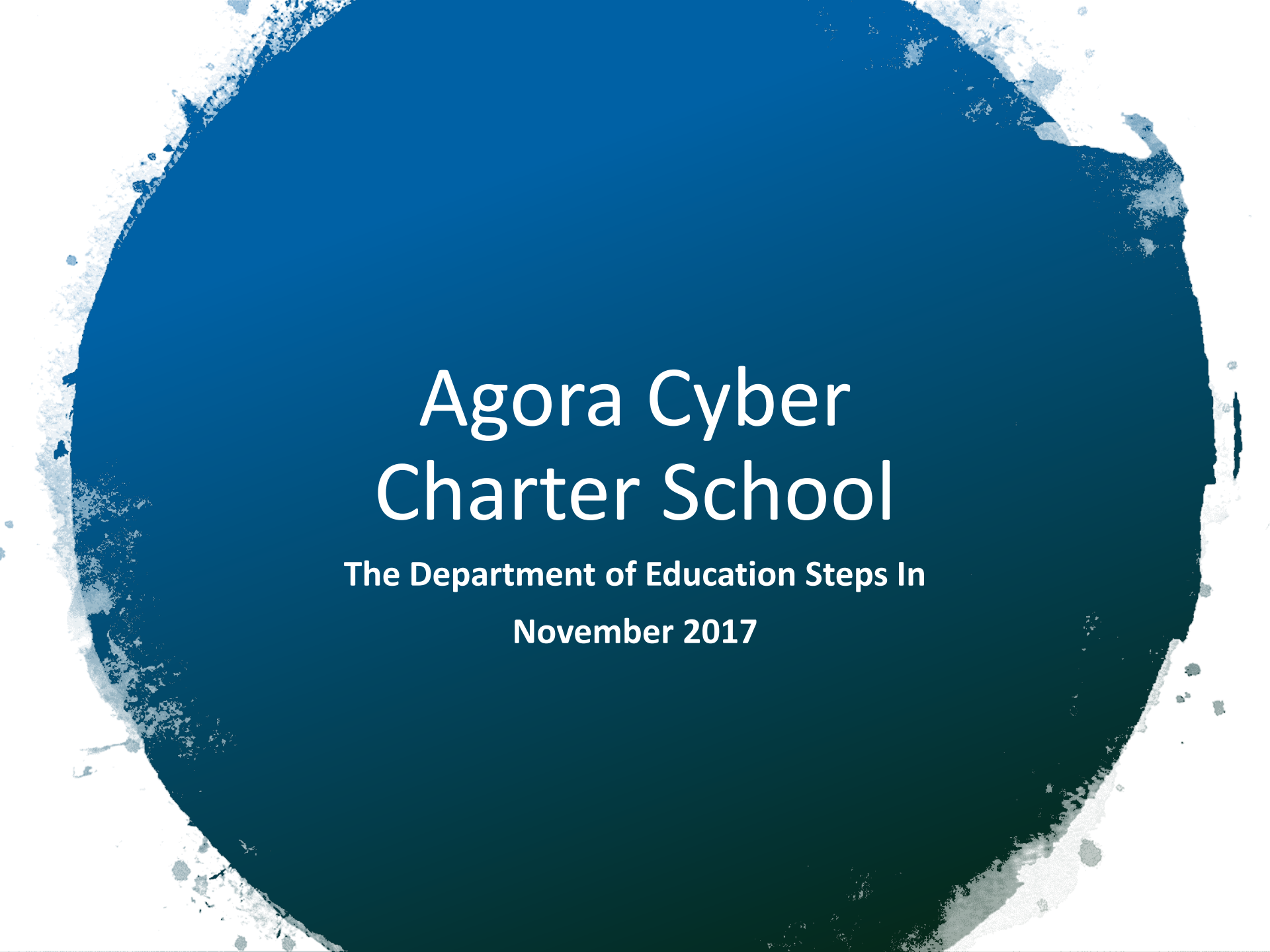
- In 2017, the Minnesota Legislature considered the Student Data Privacy Act HF 1507.
- Required:
 - A log-of-use record for any access to student data.
 - Annual training on privacy
 - Would make tech providers subject to MGDPA
 - Prohibits any commercial purpose of educational data
 - Requires notification to parents (& opportunity to inspect) every tech contract at the beginning of the year
 - No penalty for opting out of tech contracts

Future State Legislation

- Problems
 - No commercial use means – no school photos
 - Requiring disclosure of security practices – makes that data available to bad actors
 - Opt out is inequitable.
- Applied only to K-12
- Didn't advance, but expect more in the future

Future Federal Regulation?

- *Ban the sharing, storing, and sale of student data:* Several investigations have revealed that educational technology companies, for-profit schools, and other educational entities are selling student data to corporations. My plan would extend the Family Educational Rights and Privacy Act (FERPA) to **ban the sharing, storing, and sale of student data that includes names or other information that can identify individual students**. Violations should be punishable by civil and criminal penalties.
- *Direct the FTC to crack down on anti-competitive data mining practices by educational technology companies:* Big companies like Facebook and Google, and smaller companies like Class Dojo, have already collected student data to market products or to sell themselves to companies that can do so. As president, I would direct the FTC to crack down on these anticompetitive data mining practices by technology companies engaging in these practices in the education space, including by reviewing and blocking mergers of companies that have taken advantage of data consolidation.



Agora Cyber Charter School

The Department of Education Steps In

November 2017

Federal Enforcement Under FERPA: Letter to Agora Cyber Charter School

- The Family Policy Compliance Office (FPCO) issued a letter to the Agora Cyber Charter School (Philadelphia-based online K-12 school)
- Two allegations by a parent that they were forced to agree to the “Terms of Use” and “Privacy Policy” of Agora’s contractors: K12 Inc., Sapphire, and Blackboard.
- An “eligible student cannot be required to waive the rights and protections accorded under FERPA as a condition of acceptance into an educational institution or receipt of educational training or services.”

Federal Enforcement Under FERPA: Letter to Agora Cyber Charter School

1. Agora shall no longer disclose education records or PII from education records to K12 Virtual and K12 or to any other third party servicer as long as the third party servicer includes a licensing provision in its terms of use that (i) parents or eligible students are required to accept to apply for or receive educational training or services; (ii) covers “Registration Data” or other information that would constitute PII from education records; and, (iii) grants the third party servicer, its affiliates, or its licensees the “right to use, reproduce, display, perform, adapt, modify, distribute, have distributed, and promote [such covered] content in any form, anywhere, and for any purpose.” (Agora’s 2015 Response, Exhibit B, K12 Terms of Use, page 4).
2. Agora shall no longer require, as a condition of attendance or receipt of educational training or services, parents or students to accept or enter into any agreement, such as a terms of use or terms of service, with any contractor or other third party that is acting for Agora as a school official with legitimate educational interests in performing outsourced institutional services or functions that waives the rights and protections afforded to the parent or student under FERPA.

Please provide the above outlined assurances within 30 days from the date of this letter.

Efforts at Self-Regulation

- The 2014 Student Privacy Pledge
 - <https://studentprivacypledge.org/privacy-pledge/>
- Currently 395 signatories
- Applies only K-12
- Voluntary, but legally enforceable by the FTC – who can bring civil enforcement actions against companies who do not adhere to their public statements of practice
- No other enforcement mechanism
- Companies have to re-commit every year
- Will be updated in 2020

Efforts at Self-Regulation

We Commit To:

- X** Not collect, maintain, use or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student.
- X** Not sell student personal information.
- X** Not use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students.
- X** Not build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student.

Current Privacy Encroachment on Campus

- Stationary cameras in public spaces
- Body cameras on security
- Swipe cards
- Automatic vehicle recognition software in parking
- Wi-Fi tracking
- Web filtering
- Web advertising tracking
- Social media monitoring
- Thumbprint scanners or other biometric readers
- Learning analytics



The Big Technological Questions



Can We?



Should
We?

Technology Today

- Technologists are rewarded for their technical skill rather than their sensitivity to power and its abuse; and despite any gap in sensitivity it is the technical who determine the rules of technical products and whether these rules will be communicated in full to users.
 - Kate Losse, The Male Gazed: Surveillance, Power and Gender, *Model View Culture*, January 13, 2014
<https://modelviewculture.com/pieces/the-male-gazed>

Who Is Making (Conscious) Decisions About Privacy?

- “Institutions must analyze the pros and cons of data and analytics based on the local culture, values, and risk tolerance.”
 - SPARC https://sparcopen.org/wp-content/uploads/2019/10/2019_EDUCAUSE_SPARC_Poster.pdf

The Future is Here: SpotterEDU

Technology

Colleges are turning students' phones into surveillance machines, tracking the locations of hundreds of thousands



Syracuse University is among the dozens of schools in the United States that use tracking systems to monitor students' academic performance, analyze their conduct or assess their mental health. (Carolyn Thompson/AP)

By **Drew Harwell**

Dec. 24, 2019 at 7:00 a.m. CST

When Syracuse University freshmen walk into professor Jeff Rubin's Introduction to Information

- Campus-wide Wi-Fi and other sensors track student locations precisely across campuses.
- Schools give the app students' full schedules and the app can email a professor or advisor if a student skips class. Advisors also get a full timeline of a student's day.
- Students can be split into groups, e.g., "students of color" or "out of state students" for further review.

The Future Is Here: Degree Analytics

- Student's laptop or phone connects to Wi-Fi network
 - Movements are tracked around campus from the cafeteria to the science lab to the library and the dorm
 - Logs and analyzes every time a student connects a device
 - Spots patterns, e.g., when a student starts skipping class or stops coming to the dining hall.

The Future Is Here: Canvas

- When a student logs into a learning management software required by a school
- And also logs into a personal Gmail account opened in the same browser (tied to their personal identity)
- Researchers have observed Gmail (Google)'s ad tracking cookies getting synced with the LMS's Google analytics' tracking ID.
- The same tracking cookies that show you that backpack you once searched for on every website are also accessed when a student logs into their LMS.
- <https://www.funnymonkey.com/2019/personal-email-school-required-software-and-ad-tracking>

The Future Is Here: FanMaker



Orwellabama? Crimson Tide Track Locations to Keep Students at Games

Coach Nick Saban gets peeved at students leaving routes early. An app ties sticking around to playoff tickets, but also prompts concern from students and privacy watchdogs.



Alabama Crimson Tide fans at a game on Saturday. A new app tracks when students leave a game early. John David Mercer/USA Today Sports, via Reuters

<https://www.nytimes.com/2019/09/12/sports/alabama-tracking-app.html>



- FanMaker tracks student fan activity for college teams. It collects data on attendance, expenditures, movement through venues.
- Tide Loyalty Program – students earn 100 points for attending a game and 250 points for staying until the fourth quarter.
- “Privacy concerns rarely came up when the program was being discussed with other departments and student groups.”

The Future is Here: Capture Higher Ed

- Capture Higher Ed (2019)
 - Washington Post investigation found Capture Higher Ed tracking software on 33 university websites. Uses cookies to track every click a student makes on university's website.
 - Capture Ed uses software tools to match the cookie data with a student's real identity (using links inside marketing emails sent by a college)
 - Software creates data repositories on prospective students and gives students a score from 1-100.
 - Test scores, zip codes, high school transcripts, academic interests, web browsing histories, household incomes, ethnic backgrounds
 - 30 of 33 schools did not explain how they used web tracking software. At least one school said it “does not use cookies.”

The screenshot shows the Statesman newspaper website. At the top, there is a navigation bar with the Statesman logo, a 'Subscribe Now' button, and an 'ENTER TO WIN' banner. Below the navigation bar, there are several news snippets with small images and text. The main article is titled 'Colleges secretly rank prospective students based on their personal data'. To the left of the article is a 'MOST POPULAR' section with four items. Below the article is a 'Never Miss A Story' section. The article text discusses how the University of Wisconsin at Stout used tracking software to monitor prospective students and their activities on the school's website.

Statesman [Subscribe Now](#) **ENTER TO WIN**
THE ULTIMATE 2020 FITNESS PACKAGE

Man accused of kidnapping woman at student apartments in Southeast Austin, police say  Amid Texas child flu deaths, strain of virus making deadly comeback  Sheriff warns Teravista neighborhood after coyote bites barefoot man 28-story ct downtown

Colleges secretly rank prospective students based on their personal data

MOST POPULAR

- 1 Abbott says Texas won't accept refugees in 2020
Jan 10 at 2:28 PM
- 2 Round Rock officer adopts dog dragged from truck
Jan 13 at 5:30 PM
- 3 Best of prep: American-Statesman's 2019 All-Central Texas football team
Jan 10 at 2:09 PM
- 4 Beto is back: O'Rourke aims political star power toward flipping Texas House
Jan 13 at 12:03 PM

Never Miss A Story
Subscribe to Austin American-Statesman

By The Washington Post
Posted Oct 14, 2019 at 5:22 PM
Updated Oct 14, 2019 at 5:49 PM

[f](#) [t](#) [e](#) [s](#)

To learn more about prospective students, admissions officers at the University of Wisconsin at Stout turned to a little-known but increasingly common practice: They installed tracking software on their school website.

To learn more about prospective students, admissions officers at the University of Wisconsin at Stout turned to a little-known but increasingly common practice: They installed tracking software on their school website. When one student visited the site last year, the software automatically recognized who she was based on a piece of code, called a cookie, which it had placed on her computer during a prior visit. The software sent an alert to the school's assistant director of admissions containing the student's name, contact information and details about her life and activities on the site, according to internal university records reviewed by The Washington Post. The email said she was a graduating high school senior of Mexican descent in Little Chute, Wisconsin, who had applied to UW-Stout.

The admissions officer also received a link to a private profile of the student, listing all 27 pages she had viewed on the school's website and how long she spent on each one. A map on this page showed her geographical location, and an "affinity index" estimated her level of interest in attending the school. Her score of 91 out of 100 predicted that she was highly likely to accept an admission offer from UW-Stout, the records showed.

The Future Is Here: Capture Higher Ed

- Washington Post comments:
 - “This is completely creepy.”
 - “Horrrifying”
 - “One more example of our collective loss of privacy.”
 - “Mass surveillance of 17-year old American teenagers to improve the bottom line of your supposedly nonprofit institution is morally corrupt, full stop.”

The Future Is Here

- Anonymized Wi-Fi Data Is Still a Privacy Threat
 - Transport for London collected the MAC addresses of smartphones using its Wi-Fi nodes over four weeks.
 - If Wi-Fi was on, even if you were not logged in, your travel data was harvested.
 - If matched against other data sets, e.g., the travelcard system, the data can identify at the level of an individual.
 - Four pieces of data are enough to identify an individual.

The Future is Here: COURSERA

- Coursera had students type, “I certify this submission as my own work completed in accordance with the Coursera Honor Code.” It then logged all keypresses and depresses.
- Keystroke dynamics are a type of biometric credential. Considered very sensitive because, unlike a password, they cannot be changed.
- Biometric credentials
 - Facial recognition
 - Fingerprints
 - Voice recognition
 - Keystroke dynamics
- Should we make students give these things up to vendors?

The Future is Here: Pearson

- In 2017, Pearson conducted an experiment on 9,000 students without their knowledge or consent.
- Embedded “growth mindset” and other psychological messaging into its learning software programs. e.g, “Some students tried this question 26 times! Don’t worry if it takes you a few tries to get it right.”
- Pearson then tracked whether students who received the messages completed more problems than students who did not.
- Pearson claimed this was not a psychological test but a “product test.”

Privacy “Fails” Are Often Not Technical

- Instead, they are “non-technical mistakes that resulted in a disruption of social expectations”
 - danah boyd, "Making Sense of Privacy and Publicity". SXSW, March 13, 2010
- “The outrage over privacy leaks and snooping is largely because it comes as a surprise. It's not what we signed up for and not what we expected.”
 - Seth Godin, What Happens to Privacy, March 8, 2014

Other Privacy Problems: Equity

- Student surveillance – vehicle recognition, 24/7 social media monitoring, and facial recognition in the name of “threat assessment”
- Most perpetrators of school violence have been current or former students who would not alarm any such system.
 - Facial recognition Algorithms misidentify blacks at rates 5 to 10 times higher than whites.
 - “Aggression detecting microphones” that can pick up anger in a human voice have an unknown impact on marginalized populations

Other Privacy Problems: Equity

- Huntsville, Alabama (K-12)
 - Paid \$150,000 for a social media monitoring program
 - 600 accounts investigated, 14 students exposed
 - 12 of 14 (85%) were African American even though they made up only 40% of the student body

It Won't Work for Long

GIZMODO | We come from the future

LATEST REVIEWS SCIENCE IO9 FIELD GUIDE EARTHER DESIGN PALEOFUTURE

How to (Hypothetically) Hack Your School's Surveillance System



Whitney Kimball
12/27/19 4:40PM • Filed to: TUTORIALS

15.7K

15

3



Image: AP

This week, hacktivist and security engineer Lance R. Vick tweeted an [enticing](#)

Other Privacy Problems

- There's always a risk to collecting and maintaining data.
- Collecting and storing data that we don't have an immediate need for increases the likelihood of a data breach.
- A breach of this type of surveillance data would be very intrusive.



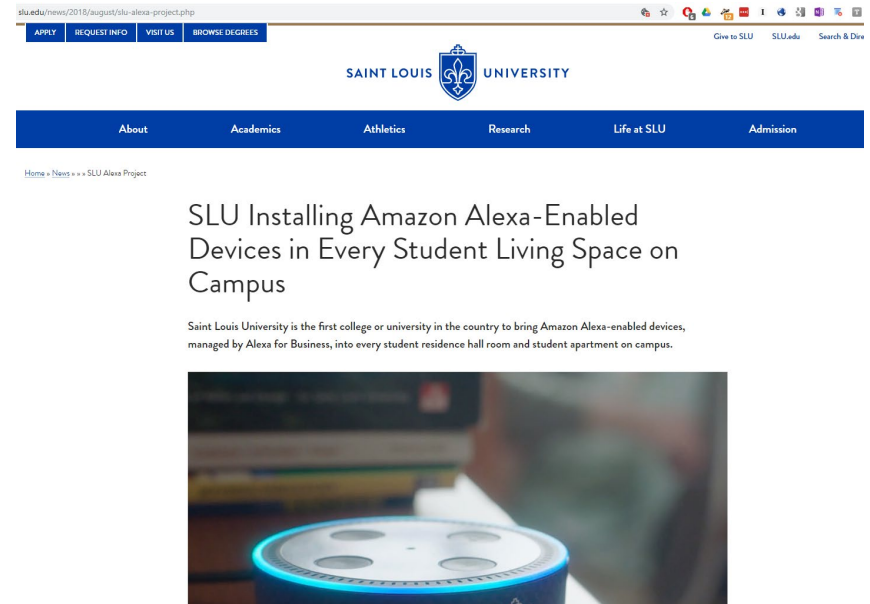
WHAT WOULD YOU DO?

Firstbeat Sports Monitor – What Would You Do?

- Finland-base company
- University athletics department wanted to collect data on student athletes' heart rates and sleep patterns, by having the athletes wear FirstBeat sensors which would send the information wirelessly to a laptop through a low energy Bluetooth connection.
- The contract said: “Customer warrants that the customer has obtained all consents and permissions necessary ... for collecting, processing, and storing the data concerning the individuals to be tested.”

Amazon Alexa in the Dorms: What Would You Do?

- Campus wants to put an Amazon Echo Dots in the dorms and develop a “skill” where students can ask campus-related questions like: what time is the basketball game? Where can I eat on campus right now?
- News reports say that thousands of workers are listening to Alexa’s recordings including background conversations.



Facebook Pixel: What Would You Do?

- Facebook Pixel is an advertising tracker
 - The pixel code in a FB ad allows FB to track how many of people who clicked a specific advertisement actually register for an event, download a report, take a survey, etc.
- While the data we get from Facebook is anonymized, you can be sure that Facebook itself gets identifiable data based on our ads. They know who their users are.
 - If we allowed this type of ad tracking, Facebook would know who did what on our campus websites, and it most certainly would use that information in the future to target advertisements to those people.
- Is it worth it? Who decides?



Who is thinking
about student and
employee privacy
on your campus?



Who is Thinking About Privacy on Campus?

Admissions?

Marketing?

Faculty?

Academic Technology?

Public Safety?

Library?

Institutional Research?

Information Technology?

IT Security?

Athletics?

Students?



What Else Can You Do?

Conduct a Privacy Audit

- What Information do you have personally?
 - In your office
 - On your phone (if shared)
 - On your home computer
 - Via shared folder (One Drive, DropBox)
 - Accessible via automatic log-in
- What information does your department collect?
 - What information do we share with others?
 - Are we collecting data for a purpose?
 - Or are we collecting data for the sake of doing so?
 - Can we purge that data?

Conduct a Privacy Audit (cont'd)

- Where does the data flow?
 - What's in the privacy policy of that third-party provider?
- Who's in charge?
 - Who is responsible for decision-making regarding data collection, use, access, sharing, and security, and use of online educational programs?
 - As a department? Campus? System?
 - Who can say no?
- How will we revisit this regularly?

Develop a Statement of Privacy Values

- UC system authored a comprehensive Statement of Privacy Values:
 - <https://www.ucop.edu/ethics-compliance-audit-services/files/compliance/uc-privacy-principles.pdf>
- University of California developed a set of principles and practices for the use and handling of learning data (a subset of student data).
 - Assumes student & faculty rights are protected contractually, learning data are secured technically, and that access and use are controlled through existing policy and processes.
 - As with grades and other sensitive data, uses of learning analytics should be pursued on a “need to know” basis.

University of California: Learning Data Privacy Practices

1. **Ownership:** Service providers will recognize learning data ownership and access as a right of the faculty and students.
2. **Usage Right:** Through a user's profile setting, service providers will enable users to control the use of their intellectual property. Thus, it will be the user's choice to grant terms such as, "a royalty-free, transferable, perpetual, irrevocable, non-exclusive, worldwide license to reproduce, modify, publish, publicly display, make derivative works."
3. **Opt-in:** Other than those data elements distinctly required for instruction, where appropriate, students will have a choice about the use of learning data collected by faculty and service providers in an "opt in" rather than "opt out" approach.
4. **Interoperable Data:** Service providers will provide learning data to the institution in recognized standard interoperability format(s) to minimize integration costs, support cross-platform and cross-application uses, and promote institutional and academic analysis and research.
5. **Data without Fees:** Service providers will not charge the faculty, students, or other university learning data stewards for the right of access, including the delivery of these data to the University.
6. **Transparency:** Service providers will inform the UC about the learning data they collect and how these data will be used, which in the course of an academic term shall be based on pedagogical concerns and curricular improvement.

Ask the Big Questions

- What kind of world do we want to live in?
- Do we care about the welfare of our staff and students?
- Is it appropriate for us to incentivize students to give up their privacy? (e.g. t-shirts for location data)
- What are we teaching our students? Are we pushing acceptance into a world of 24/7 surveillance?

We Should Be Leaders in Privacy

- Our mission is to educate
- Even if students “don’t care” we should teach them why they should care
- We should also consider potential harms of persistent surveillance on their behalf
- “But academe is supposed to stand separate from the marketplace, and be driven by loftier ideals — student autonomy among them.”

<https://www.chronicle.com/article/Students-Under-Surveillance-/247312>

Questions & Answers

- Please Chat in your questions to the host or the panelists.

How To Access Today's Materials

- Within a few business days, the recording link and PDF PowerPoint link will be posted on the OGC website:

<http://minnstate.edu/system/ogc/index.html>

OR

- If you would like a PDF copy of the PowerPoint right away, contact Liz Hegman at liz.hegman@minnstate.edu

Minnesota State Contact Information

Sarah McGee

Assistant General Counsel

sarah.mcgee@minnstate.edu

651-201-1410

Office of General Counsel

<http://www.minnstate.edu/system/ogc/>





MINNESOTA STATE

**30 East 7th Street, Suite 350
St. Paul, MN 55101-7804**

**651-201-1800
888-667-2848**

www.MinnState.edu



This document is available in alternative formats to individuals with disabilities.

To request an alternate format, contact Human Resources at 651-201-1664.

Individuals with hearing or speech disabilities may contact us via their preferred Telecommunications Relay Service.

Minnesota State is an affirmative action, equal opportunity employer and educator.