Background Information for Editors and Reporters re Student Access to Campus Records *[8/23/23]*

Contents:

1. Sample List of System Vendors

a. Maxient: https://www.maxient.com/
b. Maestro: https://www.bocavox.com/
c. Campus Café: https://campuscafesoftware.com/
d. Capterra: https://www.capterra.com/p/66468/MAESTRO-SIS/
e. Ed Surge: https://index.edsurge.com/product/ultid/P9C8-3BEE-74F8-E477-AA/
f. I-Sight: https://www.i-sight.com/solutions/title-ix-investigations/
g. Vector Solutions: https://www.vectorsolutions.com/resources/blogs/supporting-schools-in-managing-title-ix-tracking/
h. Other

2. General Uses

a. Admissions, course registration, grading, etc.
b. Alleged academic violations
c. Alleged misuse of alcohol or drugs
d. Alleged inappropriate sexual encounters
e. Alleged bias in words or actions
f. Other alleged student misconduct

3. Potential Student Concerns

a. **Student Surveillance Systems Create a Toxic Campus and Administrative Environment.** Some of the marketing materials for the entities that sell and manage these systems actually tell administrators that their systems will help schools "win" their cases against students, fueling an adversarial and prosecutorial mindset with administrators. An adversarial system in which administrators and their staffs view students as "the enemy," and their goal is seen as a need to "win," detracts from the fundamental concept that colleges and universities are educational institutions. If a student has allegedly engaged in some wrongful activity, these should be important teaching opportunities, NOT opportunities for the school's lawyers and administrators to win at all costs.

b. **Student Surveillance Systems Chill Free Speech and Stigmatize Other Legitimate Student Activities.** The ubiquitous nature of these reporting systems chills speech by allowing easy and even anonymous reports regarding what is often protected speech and other activities, as shown in recent federal Appellate Court decisions. This is compounded by the flood of reports that administration leaders encourage and even require, leading to requests to hire more staff in order to "deal with the increase in incidents," and a vicious cycle is thereby created. It also nurtures a culture in which campus administrators and their support staffs engage in aggressive and ongoing communications with targeted students as a result of their use of the templates and timelines automatically created by the case management systems.

c. **Student Surveillance Systems Are Seldom if Ever Purged of Information.** Most schools say they don't have a process for removing these materials after a specific period of years, and in many/most cases, many schools don't even scrub a student's records after the student graduates, based on the theory that the former student might later return for an advanced degree or might apply for jobs where the prior information helps assure that a school won't be embarrassed about past incidents involving the job applicant. The result is that student profiles, including anonymous and unverified reports, may never go away.

d. **Student Surveillance Systems Put Personal Privacy at Risk.** Most schools say access to information is compartmentalized and thus is limited to specific groups for each type of information. But many staff – including other students who might serve on residential staffs – have access to at least portions of these sensitive records. They can read them, edit them and can potentially share with others information they saw in the files. For example, when counseling a student about another student, there have been cases where the residential staff (inappropriately) tell the other students that X has been under suspicion for quite a while, or that X has been known to have done some allegedly wrongful action in the past, etc. but where X never even knew these reports existed.

e. **Student Surveillance Systems Can Result in a Denial of Due Process.** Students frequently are not notified when mere suspicions, let alone actual complaints, are reported. This is especially the case when the reporting party specifically says the targeted student is not to be notified (there is typically a place on most forms where the complainant can actually specify that). The targeted students therefore have no way to know who has been accusing them, or to provide explanations and exculpatory information. This information can nevertheless be used against the targeted students in proceedings that might arise months or years later, and where the accumulation of allegations, suspicions, concerns and complaints – many possibly made anonymously – creates a potentially damning compilation of information that the accused students may find impossible to overcome given the passage of time from when the reports initially were filed. Under such circumstances, targeted students may find it easier simply to plead guilty, rather than subject themselves to a hearing where all of this information will be used against them by the school's investigators, disciplinary officers, lawyers and hearing panels. Given the time and legal costs required to rebut the allegations, students may be bullied into pleading guilty even if the charges against them are inaccurate, unfair or unfounded.

f. **Student Surveillance Systems Create Serious Confidentiality Concerns.** Most of the data is managed and stored by the system providers, NOT on the school's own servers or in the school's own cloud storage. And schools using the same system providers are often allowed to poll the files of the other schools that are using the same provider in order to find out if any of the other schools have records about a targeted student. Supposedly the inquiring school then must follow legal procedures to obtain the actual information from the other schools, although just knowing that there are records elsewhere helps a school build a case against a targeted student, and some lawyers have come to believe the information is informally and inappropriately shared at times among schools without complying with legal requirements. Hacking raises other risks of inadvertent disclosure of a student's private and confidential information.

4. Articles

Op-ed by Stanford Business School Prof. Ivan Marinovic, April 7, 2023, "DEI Meets East Germany: U.S. Universities Urge Students to Report One Another." https://www.wsj.com/articles/snitches-get-sheepskins-as-colleges-train-student-informants-dei-east-germany-bias-protected-class-f941ee11?mod=hp_opin_pos_2#cxrecs_s

"Meet the Software Company Tracking College Students' Behavior," https://www.thecollegefix.com/meet-the-software-company-tracking-college-students-behavior/

"Stanford University's Pernicious Snitching Apparatus,"
https://www.nationalreview.com/2023/02/stanford-universitys-pernicious-snitching-apparatus/

"Princeton's Bias Reporting System,"
https://www.nationalreview.com/2023/03/princetons-bias-reporting-system-is-stifling-campus/

As colleges become more Stasi-like, students live in fear of being reported,
https://www.washingtontimes.com/news/2023/feb/20/as-colleges-become-more-stasi-like-students-live-i/

Breaches of confidentiality/hacking,
https://www.studentmisconduct.com/news/jauregui-law-office-petition-to-protect-the-privacy-of-title-ix-disciplinary-records-uploaded-to-third-party-database-sharing-vendors

Criticism in The Bard (from May 1, 2012), https://bardfreepress-blog.tumblr.com/post/24859899519/the-problem-with-maxient

Loyola University of Chicago, advice to students about access to their records, although also noting the information may be redacted and apparently students may be restricted to seeing mostly cases that have been completed; also noting that records are kept for seven years, etc.),
https://www.luc.edu/osccr/studentconduct/checkyourconductrecord/

Marymount University advice to students when they are subject to a disciplinary hearing, and that communications will be via Maxient,
https://marymount.edu/student-life/health-wellness/student-conduct/student-conduct-2/hearings/

Southwest Tennessee Community College Announces New System for Managing Student Behavior (May 23, 2019),
https://www.southwest.tn.edu/stories/scoop/2019/05/maxient.php

Fayetteville State University, https://www.uncfsu.edu/faculty-and-staff/divisions-departments-and-offices/division-of-student-affairs/student-conduct

5. Sample Videos and Documents Used in Training and/or Marketing

See (1) Maxient Training Guide, and (2) How to Work a Case in Maxient. Note that some of these materials at some point may be removed from the web when coming under scrutiny.

Detailed video for managing a case in Maxient:
https://www.youtube.com/watch?v=JjY6kSkjjvM

How to move materials to others in Maxient:
https://www.youtube.com/watch?v=pr0UI_r2Uq4

How dorm staff should complete a Maxient report (taking photos of IDs, license plates, if marijuana or other drugs were present, etc.):
https://www.youtube.com/watch?v=PrmgPONyNZE

Instructions about Maxient dashboards, editing incident reports, etc.:
https://www.youtube.com/watch?v=oSdnVW5T0XU

More about completing Maxient forms:
https://www.youtube.com/watch?v=XvG22yyvldE

Many more examples can be found via searches at YouTube, Google, etc.

6. Subject to FERPA (Family Educational Rights and Privacy Act of 1974)

Very complete summary from the Student Press Law Center: https://splc.org/ferpa-what-it-means-and-how-it-works/

Model form from the Student Press Law Center: https://splc.org/ferpa-request/

From North Central University: https://www.northcentral.edu/academics/academic-catalog/notice-of-student-rights-under-ferpa/ (different schools might say they have adopted different policies and practices, but they still must be in compliance with applicable federal and state laws)

From the University of North Alabama: https://www.una.edu/policies/ferpa-notification-family-educational-and-right-to-privacy-act.htm]

University of Washington Tacoma sample FERPA request form:
https://www.tacoma.uw.edu/registrar/ferpa-students

Another sample FERPA request form:
https://www.documentcloud.org/documents/21181207-example-ferpa-request

Another sample FERPA request form:
https://www.champlain.edu/compass/academic-records-and-registration/ferpa-consent-form

7. Questions To Ask About Your College's or University's Electronic Student Record Systems

1. Are electronic filing systems that record not only student courses and grades but also information about student behaviors being used at my college or university?
2. If so, did the school develop the system internally or is the school using a vendor such as Maxient or others like Maxient (see the sample links at the beginning of this paper)?
3. What information is going into the system? For example:
   a. Accusations of academic or disciplinary concerns?
   b. Title IX accusations?
   c. Concerns about a student's mental or physical conditions?
   d. Statements about allegedly biased comments or actions a student allegedly may have made?
   e. Formal and informal comments by the central student services staff, dorm staff and/or others including reports about a student by other students?
   f. Other formal or informal comments about alleged student behaviors (for example, a student was seen drunk, seemed emotionally upset, is suspected of using drugs, etc.)?
4. How do I get to see my files?
   a. Where are my school's policies and procedures for student access set forth? Who handles these student requests?
   b. If I am not allowed to see all of my files, which ones am I not allowed to see and what is the legal basis for those exceptions?
5. If I believe or am told that there is erroneous information, false information and false claims in my files:
   a. Where should I go to request the appropriate corrections and/or that the information be deleted?
   b. If my request is denied, to whom can I appeal?
   c. What other remedies do I have?
   d. Can I as well as faculty members or others submit, on our own, information including positive reviews, exculpatory information, etc., and if so, when can we do that and how do we do that?
6. Who can input data?
7. Are filings automatically entered into the electronic record-keeping system, as appears to be the case with Maxient and others?

8. Can filings be made anonymously, as also seems to be the case with Maxient and others? By non-campus personnel?
9. If I am mentioned as a secondary party in a report about another student, is that also automatically cross-referenced to my own files?
10. Will I ever be told about the concerns or complaints that are filed about me?
11. If so, when am I supposed to be told, and by whom?
12. What recourse do I then have?
13. Are there instances when information is inputted about me, including cross-references with other files about other students, and I will not be told this is happening? What are those instances?
14. Who can see what is in my file?
    a. Anyone on the student services staff, including secretarial staff?
    b. Anyone on the dorm staff, including other undergraduate or graduate students employed as dorm staff?
    c. Disciplinary staff (dean of students, Title IX, etc.)?
    d. Campus security and/or campus police?
    e. In-house and outside lawyers, investigators, counselors and others handling a school's disciplinary, Title IX and similar matters involving me?
    f. If I am applying for a paid position (such as dorm staff, intern, etc.) at my school?
    g. Faculty writing letters of recommendation, considering hiring me as a research assistant, etc.?
15. Do all university and third parties who have access to these files sign binding and enforceable confidentiality agreements? Also:
    a. Who can enforce any breaches of confidentiality?
    b. Does the school keep records about who had access to my files and what was looked at? And if so, who in turn has access to those records about access and usage?
    c. How is the school protecting my information, including under federal and state laws about privacy and the protection of data?
    d. If the school's system is ever hacked, how will I and others be informed of the hacking and what the school is doing in response, including under applicable federal and state laws?
16. Are materials about any of my alleged statements or behaviors used by Title IX and other disciplinary staff members, hearing officers and/or hearing panels? In what ways?
17. If I am applying for employment by my school (for example, to be a dorm staff member, a research assistant, etc.), do the people and entities who screen applicants or otherwise participate in and/or make the hiring decisions have access to these files?
18. If a third party is suing me and learns of this record-keeping system, how does the school respond if the school receives a demand to produce everything that is in my file?

19. If the school is using a third-party vendor, such as Maxient:
    a. Do other schools using the same vendor have access to any information about me and, if so, what information is the other school allowed to see, including even if just the fact that there is a file on me at another school?
    b. Does the system vendor itself have access to information in the system? If so, is all identifying information about me and others automatically redacted? If so, how? If not, why not and what protections then are taken regarding my privacy and confidentiality?
    c. Is the vendor allowed to aggregate information, such as number of Title IX complaints, etc., whether by specific school, by public versus private schools, by regions or by all users?
    d. Can the vendor use this aggregate or other information in their own reports, promotional materials, etc.?
20. If faculty members, staff members or others learn that information in my file is inaccurate or false, to whom should they request that the information be corrected or deleted? What procedures should be followed?
21. How long is the information about me retained in these files?
    a. Does the information get purged upon or shortly after my graduation?
    b. Does it ever get purged?

8. Sample Forms Typically Used in Electronic Record-Keeping Systems *[copied directly from a community college website]*

MAXIENT REPORTING FORMS/COMMUNITY CONCERN REPORTING FORMS

xxx is committed to fostering a safe, positive learning and working environment where all can pursue their career or educational goals and participate in college-sponsored activities. To this end, all members of the district community are provided protection and due process of their individual rights against unfair and improper action. In addition, the holistic wellbeing of all individuals within our district community is a significant priority.

The following forms can be used to report issues within our community to ensure the above commitment is met:

Student Misconduct Reporting Form – This form should be used to report any alleged violations of the xxx Standards of Student Conduct.

Title IX and Discrimination – This form should be used to report all complaints of discrimination including: National Origin, Religion, Sexual Orientation, Ethnic Group Identification, Language/Accent Ancestry, Color, Marital Status, Disability (physical or mental), Race, Immigration Status, Gender Identity, Retaliation, Age, Veteran Status, or Medical condition.

Or incidents involving: Stalking, sexual misconduct, sexual exploitation, or sexual harassment/discrimination.

General Complaints and Student Grievance – This form should be used to report general complaints as well as student grievances regarding financial aid, course grades, or the exercise of rights of free expression/speech.

Student Support Referral Form – This form should be used to alert campus personnel to individuals who exhibit behaviors and/or warning signs that may indicate a person is experiencing difficulty and may need additional support and assistance.

Electronic and Information Technology Accessibility Form - This form should be used to report 508 Compliance complaints, concerns, and grievances.

Report of Accessibility Issues – This incident reporting form should be used to report accessibility issues while at any District owned property.

9. FERPA and Your Privacy

Click here: https://www.una.edu/policies/ferpa-notification-family-educational-and-right-to-privacy-act.html

---

Supplemental Information:

Protecting Student Privacy (U.S. Department of Education): https://studentprivacy.ed.gov/

The Student Press Law Center: https://splc.org/ferpa-what-it-means-and-how-it-works/

Notice of Student Rights under FERPA: https://www.northcentral.edu/academics/academic-catalog/notice-of-student-rights-under-ferpa/

Different schools might say they have adopted different policies and practices, but they still must comply with applicable federal and state laws.