Jonathan Swotinsky

Ethics & Computer Science

Privacy Policy Review

For this assignment, I chose to review the privacy policy for "D2L". D2L is creator of the learning management system, Brightspace, which is currently licensed by the New York City Department of Education (NYCDOE) as iLearn. The D2L privacy policy describes a variety of different ways in which Personal Information is collected. According to the D2L privacy policy, "This information may include your name, email, or other personal information." Users who sign up for their own accounts, provide their own personal information through the registration process. For organizations that have a contract with D2L (e.g. NYCDOE), the organization provides D2L with users' personal information. This immediately raises the question, at what point in time and in what ways do DOE students, families, and employees have the opportunity to see the privacy policy and make an informed decision about what information they are willing to share? Further, the D2L privacy policy states, "…Under FERPA, we are deemed a "school official" to the extent we have access to student records, and we will not use such student education records for any purpose other than to perform our agreements with you or as otherwise mandated by applicable regulations." While the commitment to use students' records only for the purposes agreed upon provides some reassurance, this also raises a question. NYCDOE employees are carefully vetted before they are able to work with students and access student data. There are background checks, fingerprints, an interview process, etc. What type of vetting takes place between NYCDOE, D2L, and the employees of D2L before D2L has access to students data? And, what data does D2L have access to? Demographic data? Special Education Data? ENL Data?

The privacy policy is vague as to where students' data is stored. It implies that data could be stored internally or with a third party. However, it does include a discussion of security protocols used to protect the data. For example, the privacy policy explicitly states, "We hold many security

certifications, and we take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure, or destruction of data. These include internal reviews of our data collection, storage, and processing practices and security measures, including appropriate encryption and physical security measures to guard against unauthorized access to systems where we store personal information." The privacy policy notes that D2L and third parties follow established standards for data security, specifically the EU-U.S. and Swiss – U.S. Privacy Shield Framework.

Regarding who has access to data, the privacy policy notes that not all D2L employees have access to students' personal information. Specifically, it states, "We restrict access to personal information to D2L employees, contractors, and agents who have a need to know that information in order to process it on our behalf. These individuals are bound by confidentiality obligations and may be subject to discipline, up to and including termination, as well as civil action and criminal prosecution, if they feel to meet these obligations." However, the privacy policy does not provide a 100% guarantee, noting shortly afterwards, "We do not guarantee that we will eliminate all risk of misuse of, or unauthorized access to, your person information. There is no such thing as perfect security…"

In addition to D2L employees, the privacy policy also states that third party companies may have access to students' personal information, noting "…Personal Information collected through Brightspace or other D2L offerings and D2L websites may be stored and processed by us, our affiliates, or our service providers in Canada, the United States, Ireland, Australia, Singapore, or other countries…" The privacy policy further notes that "the laws of the jurisdiction in which the information is stored and processed will apply to its storage and processing." This raises some additional questions. For example, where are companies with access to students' personal information located, and are the laws of those countries adequate in relation to protection of personal information?

In relation to how long data is stored, the privacy policy does not state a specific length of time. Rather, it notes "if you are an enterprise user, retention of your personal information is governed by the

privacy policies and is the responsibility of your organization…[and]…subject to our contractual agreement with your organization." For NYCDOE, this means that the department of education sets the policy for how long personal information is retained as part of their contract with D2L.

The D2L End User License Agreement (EULA) is challenging to understand as an educator, and likely almost impossible to understand as a student. It is not only long (23 sections). It is also saturated in technical legal terminology. While this is not uncommon for EULA's, and while it has even become common practice for many of us to agree to EULA's without even reading them, this is a different situation. NYCDOE employees and students are "agreeing" to the EULA by nature of the fact that they are users. NYCDOE has consented on their behalf. They have not been given the opportunity to opt out.

If I were the parent of a student in NYCDOE, my first instinct would be to rely on the department of education as well as the school itself to vet the various systems used to support student learning, including iLearn. Having reviewed the privacy policy, there are some elements I would be more amenable to. For example, the idea of NYCDOE having a say in how long data is retained would make a lot of sense to me. After all, that data is what would justify my child's needs, progress, and grades. However, there are other parts of the privacy policy that I would find concerning. For example, in addition to some of the items discussed above, the privacy policy states, "Like most web sites, we use technologies, such as cookies and web beacons to collect information about the pages you view," and D2L's cookie policy includes "Targeting or advertising cookies" among other cookie types used. If I were a parent, would this leave the door open to my child receiving marketing messages on other websites because they are using iLearn? This would definitely concern me. Finally, the privacy policy notes, "We do not knowingly collect any personal information from individuals under the age of 13…" If I were the parent of a high school student, I would ask why that same level of privacy is not granted to children aged 14 – 17.

If I were a student in NYCDOE, my initial instinct may be to prioritize user experience over privacy. However, given a clear explanation of the privacy policy contents, there are some items that I would find concerning as well. For example, the privacy policy states, "by…sharing personal information with others (including sensitive information) using a Brightspace or other D2L offering or D2L website, you expressly and voluntarily consent to the storage and processing of that personal information…" This would mean that if I send a personal message to a friend on iLearn, D2L has the right to store and process that data, including but limited to sharing it with third party affiliates. From a student point of view, that would feel like an invasion of privacy, especially if I have not been given access to consent to, understand, or even see the privacy policy. This highlights the more general importance of familiarizing students with privacy policies and EULAs, how to find them, and most important how to make sense of them.

One final item to consider is how D2L makes a profit. In an article shared earlier this semester, Jaron Lanier suggested that "anytime you are provided with a service, like Facebook, for free, you are in fact the product being sold." (Baron, 2020). This provokes the question, whenever we use a free program, software, or app with our classes, are we allowing our students to become products? To the best of my knowledge, this is not the case with D2L. It is my understanding that D2L makes a profit by licensing their software to schools, organizations, etc. However, there is nothing in the privacy policy that explicitly states whether or not D2L makes a profit in other ways. For example, it seems reasonable to ask, is it possible that D2L is paid for the marketing cookies referred to above, and if so, is that a way of turning students into products?

REFERENCES

Baron, Z. (2020, August 24). *The conscience of silicon valley*. GC.

https://www.gq.com/story/jaron-lanier-tech-oracle-profile?utm_source=pocket-newtab

Brightspace End User License Agreement. (2016, April 14). D2L: Desire 2 Learn.

https://www.d2l.com/legal/brightspace-eula/

D2L Cookies Policy. (2020, February 7). D2L: Desire 2 Learn.

https://www.d2l.com/legal/cookies-policy/

D2L Privacy Statement. (2020, November 1). D2L: Desire 2 Learn.

https://www.d2l.com/legal/privacy/#site-list