Beyond HTTPS and the Cloud:
Building a Safe and Secure Web Resource for DACA and Undocumented Students

by Kenna Warsinske
(she/her)
Analyst Programmer 2,
Valley Library,
Oregon State University
warsinsk@oregonstate.edu

Kenna Warsinske (she/her) is an Analyst Programmer 2 (website developer) for the Valley Library at Oregon State University. She also volunteers to provide digital privacy and technical support for activists and local politicians. Kenna built her very first website in the small computer lab at her middle school library.

In 2016 and 2017, after the election of Donald Trump, the Deferred Action for Childhood Arrivals (DACA) program was in danger of being suspended or revoked entirely. This left many Oregon State University students in legal limbo, impacting their success as students as well as their ability to pay for college. The Department of Homeland Security, especially the small department Immigration and Customs Enforcement (ICE), ballooned in influence with the new administration. Trump had made anti-immigration a cornerstone of his campaign and that did not slow down once he took office. Undocumented students were now staring down new legal and financial challenges that were well outside their (and university) control. The university needed to respond quickly to changes in immigration policy, aid students who were struggling, and have one central location for advisors and students to find resources.

The Oregon State University (OSU) library got involved in the university's effort to help DACA and undocumented students. At the time, relevant resources were siloed across campus, so it was difficult for students to know what resources were available. Even advisors couldn't navigate the various systems. For example, on the OSU website, the Admissions page and Student Legal Services page both had relevant information, but they didn't refer back to one another. To help resolve this problem, the library offered to gather the resources distributed across campus for undocumented and DACA students.

After the resources were collected, I was approached by one of the librarians on the project to develop a more permanent technical solution. I'm a website developer for the OSU Valley Library. Just like most smaller libraries, the Valley Library relies on third-party vendors for many services; however, my department also creates custom web solutions for the library. Because this project required special privacy and security provisions for this vulnerable student population, the library opted for a custom solution.

Determining the Website Goals

First, some risk assessment was needed. This population of users might be constantly worried about a sudden change in status (such as losing DACA status and becoming undocumented), loss of employment, being detained, or being deported to a country where they might not speak the language—all while trying to go to college. That's a lot to worry about.

The users also needed to be able to trust the source of the data. Federal guidance on how to navigate the immigration and DACA system was changing almost weekly and paperwork was taking longer and longer to process. Students would need to be able to access the most recent information quickly.

Students also might not discuss their status and many campus systems are set up deliberately to not collect this information, which is good. However, students might be struggling and no one at the university would ever know. The students needed a safe and reliable way to reach out to advisors who could help them.

Given these conditions, there were two big questions, or goals, for this new website and its data:

- Would students be safe to visit the website?
- Would the resources stay accessible online?

Before I get into specifics, I'm not claiming my solution is keeping all the students' data absolutely safe from any potential threat. That's not possible. My intention is to keep this website from being an access point to vulnerable students by parties outside of the university. Also, I can't share certain information about specific security measures, but I hope to paint a general picture.

Building the Website for Optimal Security

The decision was made to develop and host a website onsite at the library. Everything would be developed by me and hosted on a custom server built by the library's server administrator. The original plan for the site was a basic "pamphlet" site with information about the new Dreaming Beyond Borders resource center, campus DACA and Undocumented policies, a list of advisors who could help, and possibly a blog. Including a blog meant I would need to step up internal security and think hard about passwords and information about registered website editors that would need to store at least a password, a username, and an email address. The blog never happened, but I still made many security and privacy decisions to protect potential website editors.

I decided to use Drupal, an open-source website builder which is similar to WordPress. In this context, "open source" means I can see and edit all the code that the program uses. If the program has code that I don't want, I can delete it. This isn't possible in third-party vendor software being used. For example, Springshare LibGuides is a very convenient website builder, but if I decided I didn't want Springshare to use a particular line of LibGuide code, I wouldn't be able to delete it myself. Additionally, if Springshare were to introduce more invasive tracking into their system, I might never know. This would be true of any closed-source proprietary software or third-party vendor. I wanted to control the code.

I also control the encryption of our Drupal database. Usernames, passwords, emails, and other personal information of content creators are encrypted (basically, scrambled) on the database, so if someone got access to the database, the hacker would not be able to see the personal information. Many data breaches you hear about in the news are just stolen databases in which a company stored personal information in a database without encryption. If a hacker

accessed the database, they could get the contact information of the website editors, which could include DACA and undocumented students who added content to the site.

Hosting the Website Internally for Accessibility and Control

The Valley Library hosts the website internally. Most campus websites are hosted in a centralized location. However, opting for extreme privacy, this site was not to be on any third-party cloud hosting providers such as Amazon Web Services or Acquia, a popular Drupal hosting provider. "Cloud" is just a fancy name for "someone else's servers," rather like how a rented storage unit is basically "someone else's garage." The cloud and storage units often have features you don't have at home, but at the end of the day, you're just a tenant. A hosting provider is able to see what websites are hosted on their platform and can decide whether or not it wishes to host it. This can make the news when big websites are removed by their hosting provider for hate speech or violence, such as when Parler was booted off of Amazon Web Services (Hern, 2021), but hosting companies also ban websites that have illegal content. Acquia specifically bans "Illegal, Harmful or Fraudulent Activities" (Acquia, Inc., n.d.) and DACA could have been considered a legal gray area. Hosting services can also ban sites just because they don't want to host the content. There might not be a reason. Sometimes they even monitor the sites on their platform. A goal for this site was to keep it "live" for as long as possible and to control any monitoring.

Avoiding Data Collection and Profile Mapping

The site was to look and feel like all other official university websites. To this end, the official Oregon State University website theme was used, but without integration with Google Analytics. Google Analytics can be very useful for developers and site owners to get a sense of the user behavior on the site, but it also builds a profile of each user, such as personal interests, hobbies, and political leanings based on their search and browsing history (Google, 2021). Google collects data indiscriminately, so I didn't want to hand Google information about visitors to this site. Again, my intention is to keep this website from being an access point to vulnerable students by parties outside of the university. Also, I didn't really need to know much about who was accessing my site. I knew I could just check with the resource center to learn if users found the layout confusing.

I also removed integration with the Oregon State University's centralized Profiles data. When students logged in to update the site, they were not connected to their centralized university profile.

Ensuring Security and Privacy with https

Finally, the https secure protocol was enforced everywhere on the site. If you're looking for the bare minimum for security and privacy for your own sites, insist on https rather than just http for your website. The "s" stands for "secure." The use of the https secure protocol protects information that travels over the internet, even from your internet service provider. Without https, your internet activity can be seen by anyone with access to your network, such as your internet service provider, your IT person, or anyone else using your same Wi-Fi network. Your internet activity includes email messages, email addresses, passwords, searches, URLs, form content, and so on. Https stops strangers and internet companies from easily scraping your data.

Meeting the Website Safety and Accessibility Goals

So let's think back to the original questions.

Would students be safe to visit the site? The site (https://undocumented.oregonstate.edu) looks identical, on the surface, to other websites across the university, but behind the scenes, every aspect of the website is controlled by the library's small team of developers. I can see all the code and I know what the site does from top to bottom. It is also hosted on the Valley Library's own on-site servers. There's no cloud in which someone else could boot the site off the internet. There are no mystery services that provide minimal functionality for the right to "datamine" visitors. The site is disconnected from third-party providers and has standard modifications for extra security.

Would the resources stay accessible online? As long as the library wants to host the site, it will remain accessible to students. From a legal standpoint, Oregon State University is in Benton County, Oregon, which is a sanctuary county, so it is unlikely that there would ever be local laws against providing information to DACA and undocumented students (Benton County, 2016).

From a technical standpoint, there's always a slim chance that certain kinds of hacks could take the site offline. Contingency plans are in place for if that ever became a problem. Unfortunately, those plans would involve temporary involvement from third-party software, which might slightly undermine the site's safety goal. In that case, the plan includes adding a statement explaining the situation and probably a Warrant Canary, that is, a message which informs students that we have *not* received a subpoena or request for data (Wikipedia, 2021). Luckily, it hasn't come up.

Libraries need usage metrics and assessment data, but you also don't want to open the door to let others mindlessly mine your students' data. This is a delicate balance. Assess the risks for the student population you're serving. Make an intentional choice before you start. Think hard about the kinds of data you need and the data you don't want others to have. As in library responses to the Patriot Act, libraries can't turn over information that doesn't exist. At the very least, make sure you have https on all of your sites.

References

Acquia, Inc. (n.d.). *Acquia acceptable use policy*. https://www.acquia.com/about-us/legal/acquia-acceptable-use-policy

Benton County. (2016, December 20). Commissioners declare "Sanctuary County." *Board of Commissioners Office*. https://tinyurl.com/2p9dkske

Google. (2021). About demographics and interests: Analyze users by age, gender, and interest categories. *Analytics Help*. *https://tinyurl.com/ywcy7pxw*

Hern, A. (2021, January 11). Parler goes offline after Amazon drops it due to 'violent content.' *The Guardian.* https://tinyurl.com/2p8jacwz

Warrant canary. (2021, November 16). In *Wikipedia*. https://en.wikipedia.org/wiki/Warrant_canary