A Study of the Collection and Sharing of Student Data with Virginia Universities

Titus Voell
Christopher Newport University

A Study of the Collection and Sharing of Student Data with Virginia Universities

Titus Voell
{Titus.Voell.21@cnu.edu}

ABSTRACT

Data collection is a vital component in any organization in regards to keeping track of user activity, gaining statistics and improving the user experience, and user identification. While the underlying basis of data collection is understandable, the use of this data has to be closely regulated and documented. In many cases, the VCDPA (Virginia Consumer Data Protection Act) outlines the guidelines for data use, data controller responsibilities, and limitations however nonprofit organizations are exempt from compliance. Colleges and universities, although still held to some degree of limitation, range in permissiveness with what data they choose to collect and retain but more importantly how and who they share their data with. This study implemented the use of open-coding techniques to look into seventeen different public and private universities in the state of Virginia. Their privacy policies were looked over and compared to the guidelines of the VCDPA to see if Universities were to follow the Data Protection Act, would they uphold the assessments and guidelines. Each of the seventeen universities collected different information and had different policies about who they shared their data too, if at all. A rudimentary scale was created to put each University in a placement. A *One* on the scale showed that the University was very conservative with their data collection and did not allow any distribution of the University's data to be shared or sold to third party companies. They followed the necessary laws from the government (i.e., turning over student documentation in the case of an investigation, etc) and reserved all other data for the University. A *Five* on the scale represented an extremely permissive policy that shared data with third-parties and that would violate the VCDPA guidelines if they were held against them. Finally, after all the information was gathered and organized, the question arose of *Should nonprofit organizations be held to the same guidelines as for-profits and why?* The findings draw attention to the gap in accountability between for-profit and nonprofit organizations, and highlight how some nonprofits have taken advantage of the deliberate inattention and freedoms given to them.

1 INTRODUCTION

For-profit organizations are defined as such: A type or organization which seeks to obtain a profit through its operations and dealings and is concerned with its own interests. These organizations, understandably, have clear lines set in front of them to protect their customers privacy and transitively their data. Companies orchestrate “sales", or “the exchange of personal data for monetary consideration by a controller to a third party”. The Virginia Consumer Data Protection Act gives the users and controllers clear rules of how for-profit organizations are allowed to go about selling and trading data. An example would be in article 59.1-578 stating, “Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes the categories of personal data processed by the controller, the purpose for processing personal data, and the categories of personal data that the controller shares with third parties, if any.” The VCDPA is all about controller transparency in order for the user to know exactly what information is being collected from them, how it is being collected/used, and where/to whom it is being sold to. Nonprofit organizations have been largely exempt from the VCDPA laws. A nonprofit organization, or 501(c) organization, is an organization where its primary activities are “charity, religion, education, scientific, literary, testing for public safety, fostering amateur sports competitions, or preventing cruelty to children or animals.” These exempt organizations have much less responsibilities and restrictions when it comes to user data. Universities have collected thousands of students' data and, although they still create privacy policies as a public statement of how they collect, use, and share data, many Universities have hid behind the nonprofit title as they share student data with third parties. Shouldn’t the protection of students’ data be inclined to be prioritized over many for-profits’ data? Should Universities be giving away student data, no matter how much? Should nonprofit organizations be held accountable the same way for-profits are to rules and regulations such as the VCDPA? The argument can be made that everyones’ data is all important and should be treated equally, however, student records, transcripts, and personal information have a big role to play in their later future and, depending on what sector each student decides to move into, that data, if a University chooses to give it away, can impact their future outside the university. Students’ data is much more valuable and important than the statistical user data gathered from a for-profit. For-profit organizations are lawfully inclined to

offer their users an “opt-out” from data collection; nonprofits are held to no such accountability. For this open-coding research topic, seventeen universities in the state of Virginia were picked to be investigated. These universities’ privacy policies and any other publicly released information about their data collection and use policies were thoroughly explored and categorized.

2 METHODOLOGY

As these universities are listed, they will be in order of their categorization of data sharing range: one to five. A *One* for a university represents a very conservative use of their students' data and, if compared to the VCDPA, would uphold all laws and regulations. A *Five* would represent a very permissive use of the university’s student data and would go against one or more of the rules and regulations set forth by the VCDPA. As we categorize the universities, we will assume that the baseline data collected consists as follows: Student full name, address, phone number, email address, social security number, academic records, financial aid information, and other student demographic information. Digital information such as IP addresses, browser type, and operating system is also a baseline for university data collection. We can assume this because, after reading through all seventeen privacy policies, this is a common trend with every policy listed. We can also assume that every university, even if they do not share any of their data with third-parties, are legally obligated to share students’ data and information as requested by law enforcement and any other verified legal situations. Any other data other than that which is listed above will be detailed below.

• **Christopher Newport University** - Christopher Newport University prides itself in very strict security policies and procedures that they have put into place to protect the privacy and security of the data they collect. On rare occasions, Christopher Newport collects health-related data such as medical history from certain students when it is necessary for specific purposes such as accommodations for students with disabilities. Overall, Christopher Newport collects and uses data and information to support its educational mission and provide a safe and secure environment for its community, while also respecting individuals' privacy and confidentiality. Given the rating of a *one*, Christopher Newport upholds all regulations outlined in the VCDPA and refuses to give or sell their students data to any third-parties.

• **Virginia Commonwealth University** - Virginia Commonwealth University uses their own university offered application called *VCU Health MyChart* app. The application collects the students’ location data even when the app is not running. The application also temporarily stores copies of the students healthcare documents as well as identifiers and times for upcoming events the student has set. All data, except for the location data, is removed from the students device after a period of time. All communication records of the student contacting the VCU health system through the app are recorded and stored. The records are also given to the VCU health system as clearly stated in their privacy policy. No other student data is shared with third-parties. This university's rating is a *one* because, even though they internally distribute records of student conversations with the health system, they are kept within the VCU health system and the use is clearly written out in their privacy policy, just as the VCDPA states it should be.

• **Norfolk State University** - Norfolk State University does not collect any extra data from their students, except to the necessary extent for the university to complete an order or request by the student, and they equally do not share or sell any sort of information or data to third parties. Although Norfolk State is very strict with their data sharing policy, their security may not be up to par. As stated in their privacy policy, Norfolk State uses social media platforms such as Facebook, Instagram, Twitter, LinkedIn, YouTube, and TikTok. Each one of these social media sites are known for their outstanding data breaches over the last few years. Through the use of supply chain attacks, universities who use social media platforms are at a larger risk of a data breach. This use of social media, however, does not violate any VCDPA regulations so Norfolk State University was given a rating of one.

• **Longwood University** - Longwood university collects bare minimum data only from students. They monitor their university website and collect statistical data such as the number of students who visit different parts of the website to make the site more useful to visitors. They are extremely conservative about data sharing policies and have very strict security even in their own university about which department is allowed to have access to certain data. A rating of *one* was given to Longwood University because of how little of their student’s data they collect and share.

• **Hampton University** - Hampton University is very similar to the schools listed above in terms of privacy. They do publicly display students' first and last names on their public profile page. This may pose a privacy problem if the university did not offer an opt-out option. Any student can either remove their name or make their profile hidden which, held up to the standards of the VCDPA, would uphold regulations. Students' credit card information can be saved on their account but is easily able to be taken off and the appropriate security measures have been implemented by Hampton University so that only the student can see their information. Once again, this university was given a rating of *one* for their conservative approach to data collection and sharing.

• **Regent University** - Regent University, although still very secure with their students’ data, explains in their privacy policy that some data is accessible to employees and partner’s employees. The data that is available to them is data given freely by the university's students. While the data is in the university's control or while in the control of

one of their campaign partners, they have ample security and policies in place to protect students' data. Regent University was rated a *one* due to their ample security and transparency.

• **Shenandoah University** - Shenandoah University's privacy policy focuses more on website data collection. They keep track of services that users interact with, they record users preferences and track pages where they visit to reveal how users travel throughout the website. The information they collect is used to improve users' experiences and help the university better understand how the website is being used. Shenandoah University does not share information with third parties and keeps all student data confidential and secure. Because of this, Shenandoah is given a rating of *one*.

• **Washington & Lee University** - Washington & Lee University is much like the first few universities in that they only collect the very basic information from their students. They have a zero sharing policy for third parties as well as multiple apt-out options for their students in terms of emails sent, website data collection, and university communication. “We do not provide any third parties with any voluntarily or otherwise personally identifiable information, meaning we do not sell, rent, or market personal data about you to third parties.”

• **James Madison University** - James Madison University goes into extremely long detail about how they share their data with law enforcement, any ongoing investigations, and accredited agencies

• **Lynchburg University** - Lynchburg University collects basic information from their students but they mention that from time to time, individuals or companies under contract with the University may have access to information in the course of the service they provide to the University. Their privacy policy does not specify who the contractors are nor what sort of data these contractors have access to. This goes against the VCDPA guidelines which say the organization must outline what categories of data third parties are allowed access to. Because of this finding, Lynchburg University was given a rating of *two*.

• **Old Dominion University** - Old Dominion University was rated *two* because, although they do not share students’ data with outside third parties, they do share data inside the university with multiple different departments. Specifically, students’ data is shared with Registrar, Career Development Services, Financial aid, Office of the Dean of Students, Office of the Dean in each of the Academic colleges and advising centers, and office of Finance. There is no information presented as to which department has access to what information which violates the VCDPA rules of transparency concerning data sharing.

• **University of Virginia** - The University of Virginia prefaces their privacy policy by clearly identifying the two types of data they collect: access information and option information. Access information consists of client information, or student information, and optional information is personal data. This information is kept secure and only used when fulfilling a request or order for students. The reason this university was given a rating of *two* was because they publicly advertised links for other companies and organizations on the university's public page but gave no indication of those links policies on data collection. After researching the third parties' links, they were found to be for-profit organizations who actively gathered and sold their users' information. The University of Virginia gave no warning and displayed their links.

• **Mary Washington University** - Mary Washington University's policy details a larger number of third parties with whom they share their students’ data with. They say that they share students' personal information with their group companies, affiliates, subsidiaries or contractors. Personal information is also shared with their third party service providers and business partners who assist with the running of the Sites and their services and products including hosting providers, email service providers and payment processing partners. Mary Washington University also retains personal information for as long as they deem necessary and does not give options for opting out or deleting personal information. The combination of oversharing student’s personal information and controlling their data without letting the student have a say in it violates guidelines set in place by the VCDPA. Mary Washington University was given the rating of *three*.

• **Radford University** - Radford University’s privacy policy looks strikingly similar to Mary Washington University’s privacy policy. Research was done as to whether there was a general Virginia template for universities to make their privacy policy but nothing came up. Either both universities worked together on it or the same third party wrote them. Radford presented their information the same way Mary Washington University did which detailed the extensive list of companies and subsidiaries who have access to students’ personal information. Because of this, the university was rated *three*.

• **Virginia Polytechnic Institute and State University** - Virginia Tech, a school known for its advanced technology and engineering programs, has a surprisingly small privacy policy. More specifically, Virginia Tech does not outline or publicly outline any type of data they collect or share from their students. The little information that they do have is website data collection; they do not collect website data. They claim they do not share any personal information, however, with the lack of transparency, the claim has no backing. Virginia Tech was given a rating of *four* because, if it was held to the VCDPA policies and regulations, it would be in violation of quite a few. This university is a clear example of how nonprofits take advantage of the fact that they are not required to follow the regulations set into place for for-profits.

• **George Mason University** - George Mason University takes every advantage they can think of without flat out selling their students’ data away. They permit third party

service providers to collect and process some information from our digital properties. They share personal information with these providers and have similar arrangements with internet-based advertisers. Additionally, George Mason University's digital properties, such as their main websites, the sites students use for classes and personal information, are not designed to respond to "do not track" requests from browsers, meaning students are not capable of limiting the information the university chooses to take. George Mason University was given a rating of *five*.

• **William & Mary University** - William & Mary University, the most permissive university that was chosen for this study, has both little transparency and what they do choose to display in their privacy policy goes against everything the VCDPA was put into place for. William & Mary University writes, "Data is shared with 3rd-party analytics and marketing tools—such as, but not limited to, tools from Facebook, Google, HubSpot, LinkedIn, SiteImprove and YouTube." Although the number of companies the university shares their data with is concerning, this alone does not violate any VCDPA regulations. The reason it would break rules is because, in order to be keeping the VCDPA regulations, that organization must alert the user (or student) prior to sharing their information with a third party. There must be ample time for the organization to contact the user and William & Mary University does not do that. Lastly, the university does not specifically the data they collect at all. They do mention that they collect data but withhold the information as to what data they gather. All this together is what makes William & Mary University rated a *five*.

From the data listed above, the results indicate that each institution has a range of sharing policies. When students choose the school they hope to attend, they often do not take into account the university's policies. Arguably, they should not have to look through all the university's policies before they make their decision which leaves the university to take accountability for protecting their students. If these institutions were to be held to the same standards as for-profit organizations, what would that look like and to what extent would they be required to limit their data sharing?

3 ANALYSIS

If nonprofit institutions were to be held to a guideline of rules and regulations, the first step would be to clearly outline for students and users exactly what data is being collected and to what extent. This seems like a simple regulation but many universities provide scarce details if any on the matter. Section 59.1-578 of the VCDPA gives a clear set of rules about transparency. It also says that controllers (the institution that is collecting data) must provide an opt-out option for having their data collected and sold/shared. "If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing." The next step would be to have universities and institutions alike limit their contact and business with third parties that are known to have loose privacy policies (i.e., the third parties sell data that is given to them for purposes other than business) and only use student information inside their institution. Non-identifying data should also be closely kept de-identified while sharing with processors so that the data can not be re-identified as to keep the anonymity of the student or user. "The consumer rights contained in subdivisions A 1 through 4 of § 59.1-577 and § 59.1-578 shall not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information."

Why should student data be so closely regulated? Although there are some exceptions, student data is critical for the students future. Records and transcripts are used to apply for internships, jobs, and scholarships. Their personal data including social security numbers, credit card information, and other personal data are extremely sensitive and important. Students put large amounts of trust in universities to secure their data so it is not released to third parties who should not have access to that level of information. Even students' emails should be securely kept to shield the student from phishing attacks and a multitude of spam emails. Universities have a public responsibility to protect students and do everything in their power to provide opportunities and paths for them. Sharing information and giving access to sensitive data to third parties who are not concerned with the students safety and privacy is why nonprofit organizations should have more accountability concerning their interactions with processors and controllers. Many nonprofits rely on public trust to operate effectively so it is not only in the best interest of the students to protect their data securely but in the interests of the universities as well.

4 CONCLUSION

Because of the large use of the internet, users' data is more than likely accessed by many different websites who actively share information and sell to a number of third parties. Many people have become desensitized to the idea of data privacy and have no interest in looking for clear signs that the nonprofit company or organization they are involved with or a part of actively keeps their information secluded and private. They place a large amount of trust in the nonprofit that their data is not being circulated around to numerous third parties. The responsibility of security then falls on the nonprofit to uphold the users' trust and actively restrict access to users' data and to keep it out of

the hands of third parties. Statistical data is one the core necessities of web development to know which site is getting more traffic and what to improve and universities already collect that to better their user experience. Most data collection is within legal boundaries, it is the moment that universities choose to give access to that data or do not clearly document for their users what data is being collected from them. For this reason, universities, and more specifically, nonprofit organizations need to have legal guidelines set in place just as for-profit organizations do to ensure they prioritize the safety and privacy of their students and users' data.

5 REFERENCES

Usercentrics. (2022, August 12). *The Virginia Consumer Data Protection Act (VCDPA)*. Cookiebot. Retrieved April 13, 2023, from https://www.cookiebot.com/en/virginia-vcdpa/

Virginia Law. (2023, January 1). Title 59.1. trade and Commerce. § 59.1-578. (Effective January 1, 2023) Data controller responsibilities; transparency. Retrieved April 13, 2023, from https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-578/

Wikimedia Foundation. (2023, March 25). 501(c) organization. Wikipedia. Retrieved April 13, 2023, from https://en.wikipedia.org/wiki/501(c)_organization

Privacy Policy. Washington and Lee University. (2020, January 1). Retrieved April 14, 2023, from https://my.wlu.edu/about-this-site/privacy-policy#:~:text=Personal%20Information&text=We%20do%20not%20provide%20any,about%20you%20to%20third%20parties.

William & Mary. (2017, January 5). Privacy & Security statement. William & Mary University. Retrieved April 14, 2023, from https://www.wm.edu/aboutthissite/privacy/