Donor Privacy or Disclosure: What's Better?

We the People, do ordain and establish this Constitution. No laws shall be made "abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble", ensures donor privacy is protected by the First Amendment. The interpretation in the Bill of Rights provides for the justification for privacy and protection in fundraising and philanthropy. Donor privacy interests must be valued in nonprofits, otherwise the legitimacy of the sector comes under question and the government will detect the need for further regulation. It is important for nonprofits to limit the dissemination of personal data with the consent of the persons about whom the information is collected. Over the past decade, many controversies regarding the ethics of donor confidentiality have arisen, such as the hacking of Blackbaud, HIPAA privacy rights, the implementation of individual state donor privacy and disclosure mandates, donor list sharing, and the historic *NAACP vs. Alabama* Supreme Court case that upheld the constitutional right for donors to remain anonymous. As a topic for conversation in nonprofit ethics, the *Principles for Good Governance and Ethical Practice* and the *BBB Standards for Charity Accountability* discuss charitable solicitation compliance protocols to ensure ethical conduct by nonprofits and to entrust public confidence. This paper will explore the commitment to donors by nonprofit organizations in maintaining donor privacy and disclosure practices based on the integrity, fairness and the intention of donor philanthropic freedom, while upholding the law.

Donor Privacy "allows charitable givers to follow their religious [or other] teachings, insulate themselves from retribution, avoid unwanted solicitations, and duck unwelcome publicity. It also upholds and protects important First Amendment rights of free speech and association" (Philanthropy Roundtable 2017, 1). In essence, forced donor disclosure can be seen

as unconstitutional as charitable giving is based on the founding fathers core values of beliefs to provide for the public welfare of mankind, freely and without constraint. Gifts have specific designations, such as categorization of size, restrictions, and the need to remain anonymous. The "Do not" lists for soliciting, mailing, calling, and publicizing are most common forms of donor privacy which should be presented to all donors during their initial gift (Scanlan 2013, 68-9). Donors have professional and personal reasons for not wanting recognition and by providing recognition of the donation value may violate privacy. Furthermore, The Center for Public Integrity maintains the following as donor essential data: contact information, giving history, event attendance, publication distribution, and program requests (The Center for Public Integrity 2020). These are filed for auditing and IRS tax exempt purposes. Similarly, the Association of Fundraising Principles (AFP) and Charity Navigator have adapted multiple donor privacy regulations to maintain donor confidentiality. AFP categorizes donor privacy as Personally Identifiable Information. They have adopted their own Donor Bill of Rights to assure donations are handled confidentially and donors are allowed to remove themselves from receiving publication information, among other privacy rights (AFP 1993). In addition, AFP's Code of Ethics sets donor privacy behavior standards that members must "value the privacy, freedom of choice, and interests of all those affected by their action" (Scanlan 2013, 60). Charity Navigator stresses the importance of accessibility and transparency in regard to donor privacy when they rate nonprofit agencies (For Purpose Law 2018). As an example, Charity Navigator represents how small and simplistic a privacy policy can be:

> Our Commitment to Our Donors
>
> We will not sell, share or trade our donors' names or personal information with any other entity, nor send mailings to our donors on behalf of other organizations.

> This policy applies to all information received by Charity Navigator, both online and offline, on any Platform ("Platform", includes the Charity Navigator website and mobile applications), as well as any electronic, written, or oral communications.
>
> To the extent any donations are processed through a third-party service provider, our donors' information will only be used for purposes necessary to process the donation. (Charity Navigator 2020)

To demonstrate consent for data privacy rules in the United States, there are longer policies that utilize a two prong approach - explicit or opt out policies to allow for trust. Explicit meaning information will not be shared without permission and when permission is sought from donors they have a right to exclude themselves from information sharing. Opt out implies an organization can automatically use a donor's information unless told not to (For Purpose Law 2018). Prospect researchers are involved in ethically maintaining donor data. *Prospect Research for Fundraisers: The Essential Handbook* shares guidelines for protecting information: shred files, never send unsecured information via email, lock files away, secure donor databases, craft a confidentiality agreement, minimize donor files leaving the office, and enforce necessary laws are just ways to avoid real harm (Filla & Brown 2013). Donors can also elect to remain anonymous, although only 1% of giving is conducted unidentified, there is a fine line between this anonymity and publicity (Schroeder 2016, 8). The most common reason for anonymous charitable giving is "the desire to avoid the deluge of giving requests that often trail major donors", as financially donor advised funds provide the largest degree of flexibility (ibid). Lauren Shenfield, Executive Director at Philanthropy Advisors recommends strategies such as establishing recording keeping safeguards, creating a board policy protecting anonymity, consulting tax professionals in the gift process, and informing staff of ethical confidentiality

practices (ibid). While donor privacy laws and regulations must be implemented to benefit and protect donors, donor disclosure rules have come under close scrutiny and contestation.

Institute for Free Speech explains three ongoing threats associated with government regulations that would require overruling donor privacy and protection rules, namely in electoral and political campaigning. Due to unprecedented political contributions over the last decade, Congress believes stringent regulations need to publicly disclose donors that have contributed over a certain threshold amount. First, "electioneering communication" regulations are too broad. They lack how to specify nonpartisanship and advocacy engagement as it relates to disclosure of financials (Nese 2015). Second, the creation of the incidental PAC would subject an organization to detailed reporting and disclosure requirements. Third, federal and state legislators may use their overreach of authority to write new requirements, garner votes, and minimize oversight. The government regulators are in a position of power to determine what reporting is and how it is enacted, which could have long lasting repercussions on philanthropic giving and donor tolerance. Recently, this issue has caused concern regarding ballot initiative measurements. Today, the United States of America "mandates more disclosure of political spending and contributions than at any other time in its history" (ibid). This causes grants to be smaller, with more ethical dilemmas arising, legal ramifications occurring, and the delegitimization of charities, while simultaneously striving for philanthropic freedom.

Ultimately, nonprofit philanthropic giving donor privacy needs to be closely monitored as donors can come under retribution if disclosures are made. This freedom is the protection and "the right of Americans to choose how and where to spend their charitable assets in order to fulfill their diverse missions" (Philanthropic Roundtable 2020). Threats to this freedom are prevalent in the 21st century as the elimination of tax deductions for certain

nonprofits organizations may shift to donors' contributions, thus preventing them the liberty of giving, without harm. The unstructured nature of private foundations may also devalue good governance. Donor advised funds are yet another threat, as disclosure of these funds and their origination is not required. In this case privacy is bad, as donors can give to "controversial philanthropic causes without fear of harassment and reprisal" (Florino 2020). State and federal legislation has eliminated some of these threats. Under the "Personal Privacy Protection Act" currently enacted in seven states, nonprofits can keep their records private, unless the law or a subpoena is enforced (Philanthropic Roundtable 2020). Furthermore, these nonprofit organizations have protection from unintentional disclosure, retribution from outsiders, and political insiders. Political partisanship has affected certain aspects of state legislation, where some states are seriously considering requiring donor disclosure. On the other hand, the federal government, thus far, has been quiet in attempting to legislate nationwide donor disclosure regulations, hoping that the Constitution and Bill of Rights is upheld to maintain donor privacy freedoms to enable nonprofits to meet their beneficiary obligations.

While most of the state donor disclosure bills have died, keeping intact donor privacy rules, it is evident that privacy regulations remain under attack. With more public support, legislation in favor of donor privacy will positively move forward, as proven through historical precedent of relevant case studies that demonstrate the need for privacy. In 1958, the *NAACP v. Alabama* was presented to the Supreme Court. There it upheld that the disclosure of NAACP's membership and donor lists threatened their freedom of association, ultimately allowing their donors to contribute anonymously. "An inseparable aspect of the 'liberty' assured by the Due Process Clause" is the advancement of ideas from nonprofits (Philanthropy Roundtable 2017). This upholds the right valued by a free people granted under the Constitution and Bill of Rights

and does not infringe on those freedoms. The Supreme Court's decision stated that vulnerability exposure could cause long term "economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility" (Parnell 2017). This ruling has been ignored to the point where Mississippi has implemented HB 1205, their version of a donor privacy law to stress the importance of free speech on the state level (Mississippi Center for Public Policy 2019). With these landmark decisions, one may think donor privacy is safe and sanctimonious. Luckily for nonprofit organizations, Philanthropy Roundtable is at the center of litigation support for donor privacy laws protecting donor freedoms (ibid). Their multitude of amicus briefs highlight the urgent constitutional concerns that could enforce legislation in support of donor disclosure.

In terms of litigation, California and New York have been on the forefront with court cases. In 2010, now Vice-President Elect Harris as attorney general was demanding that portions of the IRS 990 tax form be more public. Specifically, Schedule Bs be shared to include annual reports of major donor information as a requirement for charitable state solicitation. The office claimed it was to "protect the public against fraud", although no actual enforcement of this mandate followed (Florino 2020). Cases challenging this donor reporting such as *Americans for Prosperity Foundation v. Becerra* could finally shut down donor privacy opposition (Philanthropy Roundtable 2020). In May 2020, the Internal Revenue Service final recommendations were made ensuring certain 501(c) organizations did not have to report or disclose substantial donor information. While not subject to the provisions of the California Consumer Privacy Act which went into effect at the beginning of the year, nonprofits may fall under its influence. For example, for profit entities, consumer data, third party contracts, and commercial activity which engage with nonprofits are subject to this act. Four principles among

all California businesses were implemented to provide broad consumer rights - right to know, right to delete, right to opt-out, and right to non-discrimination (Office of Attorney General 2018). In 2006, the New York attorney general's office demanded the same filing requirements and in 2014, Citizens United sued the same office asserting that mandatory disclosure violated federal law confidentiality. This was in reaction to the infamous *Citizens United v. Federal Election Commission* case that argued about the transparency in political spending including charities later would be known as "dark money" (Philanthropy Roundtable 2017). Nonprofits and donor privacy are supposed to be nonpartisan in nature. Although, disclosure has close ties to democracy, campaign financing, and electing regulation, so it has fallen in line with progressive values, whereas privacy has come from conservative government stances (Florino 2020). President of the Mississippi Center for Public Policy, John Pritchett voices a similar belief that "many on the left oppose this bill because they want to know who funds their opposition so they can bring pressure to bear on them and suppress their speech with coercion and harassment" (Mississippi Center for Public Policy 2019). Retaliation can be expected more often when politics is involved, hence why anonymity is still important. Too much disclosure can actually cause more harm than good. This is certainly the case when it comes to the Health Insurance Portability and Accountability Act (HIPAA) privacy rights.

Similar to the concept of donor privacy, HIPAA was enacted in 1996 allowing for patients to have the right to access their health records, ensure the accuracy of their records, and know how these records are being shared. The Privacy Rule known formally as the *Standards for Privacy of Individually Identifiable Health Information* addresses the disclosure protected health information and other covered entities. This rule's minimum necessary clause has obvious comparisons to donor disclosure where an entity seeks "only the minimum amount of

information “needed to accomplish the intended purpose of the use, disclosure, or request” (Office of Civil Rights 2003). Protected health information can be used for fundraising or marketing purposes as long as HIPAA provisions continue to be met and allows for the patient to opt-out; every fundraising appeal must include an opt-out policy (AAMC 2014). Health information marketing policies are treated identically to donor contributions, but regulatory compliance appears to be harder to maintain and funding is dependent upon the successfulness of compliance and electronic data encryptions (Bryan 2016). As a result, nonprofits can lose program funding, staff, equipment, and clients. Hospitals and health for profit entities, furthermore, may put their own credentials at risk by assisting nonprofits. It seems as if every nonprofit subsector must deal with the donor privacy issue and be cognizant of changing laws to communicate impact and intentions, regardless of donor privacy and disclosure regulations.

Is donor anonymity and privacy worth protecting? Is anonymity still needed? While philanthropy is voluntary, “forcing giving to be more public is likely to damage the sector and result in less giving, not to mention infringements” on fundamental constitutional rights (Philanthropy Roundtable 2017). Databases provide access to giving information. A main issue with donor privacy is the access to this information is greater than the desired range. This range has led to a breach in security measures. If unauthorized individuals obtain access to this information, an invasion of privacy and a damage of records is likely to occur, not to mention the compromising of integrity of the nonprofit. Most attacks appear as common legitimate access, hence employees should be educated on security, database usage, and hacking schemes. In the summer of 2020, public damage to Blackbaud, a major corporation that manages customer relationship databases for nonprofits was hacked. They paid a ransom to cybercriminals and publicly revealed the occurrence of the hack in July, but did not publicly or internally disclose

the incident when it first occurred. Nonprofit users were dissatisfied to hear this hack occurred in February and was not identified until early May. The ransom paid in Bitcoin proved successful since evidentiary support showed no data was shared beyond the hacker's leverage. As Blackbaud continues to value its relationships and apologize, the affected nonprofits have the right to take donor privacy obligations seriously. Data protection is not simple, "the amount of forensic work necessary to ensure that systems are no longer infected, data hasn't been compromised, and getting to a position to credibly issue a breach report requires a massive effort and significant time and cost" (Clolery 2020a). Months later, business actually became more uncertain as Blackbaud discovered more of the hack details. This additional information pertained to sensitive data fields that were thought to be encrypted, but after further investigation were unencrypted. The general public feels the blame is being shifted on nonprofits, since the fields in question point to data input from the customer end (Clolery 2020b). Is this a moral obligation that should be accepted by the nonprofit because of poor conduct in not securing their databases? After all, how does the public know that cybercriminals actually deleted the data they were holding hostage and it is unknown if donor names could surface in the future. Nonprofits strive to care for organizational interest, while appearing donor centric with privacy and protection of primary concern, but this often leads to internal conflicts, donor distrust, poor judgement by stakeholders, and damage to the sector.

In order for trustworthiness to be upheld and the ideal of donor privacy, membership and monitoring associations have set standards. Two of these organizations, Independent Sector and BBB Wise Giving Alliance address effective governance, finances, transparent and responsibility fundraising, legal compliance and reporting, and integrity. The Independent Sector's *Principles for Good Governance and Ethical Practice* serve as a guide for all nonprofit types, listing thirty

three principles that strive to embrace the public's trust and ethical conduct. Specifically, responsible fundraising principle thirty three involves donor privacy stating:

> A charitable organization should respect the privacy of individual donors and, except where disclosure is required by law, should not sell or otherwise make available the names and contact information of its donors without providing them an opportunity at least once a year to opt out of the use of their names. (Independent Sector 2015, 43)

This language reflects the need to preserve data and disclose how donors' information should be utilized. It calls for certain safeguards to be implemented such as opt-out policies, electronic communication parameters, and creation of privacy policies for donor protection among other policy and procedural inputs. In addition, principles six and seven address the intricate balance between transparency versus privacy (7). Six sides on the err of privacy discusses asset protection, integrity, liability, and reputation to mitigate when losses occur. On the other hand, seven agree with transparency, insisting on publicizing all timely information and sharing evaluation reports (16-8). These principles conclude that donor privacy is valued in some areas, while in other areas it is frowned upon. Similarly, the *BBB Standards for Charity Accountability* evaluate whether one of their twenty standards is met, unmet, or unverifiable and list in a nonprofit's finding report (BBB Wise Giving Alliance 2003). A nonprofit's appeal to the public must be accurate and integral. In terms of solicitations and information materials, standard eighteen discusses donor privacy. To assure these concerns are addressed, BBB Wise Giving Alliance explains:

> We require that charities do two things: one is that at least annually the charity should provide direct-mail donors with the ability to opt out of having their name and address shared outside the organization; two, the charity's website should include a prominent

privacy policy that covers certain specified points about notice, access, opt-out information, and security. (ibid)

Most ethical concerns have been communicated by the guidelines established by BBB Wise Giving Alliance and Independent Sector, where it verifies the trustworthiness of charities through rigorous reporting and evaluations. These guidelines are carried forward in the Analytical Framework for Ethics, whereby outcomes, obligations, and intent to fulfill the duty of stakeholders is executed to ensure the nonprofit sector is secure.

This Analytical Framework for Ethics involving the aspects of consequence, duty, and virtue of stakeholders is necessary to provide transparency to donors to ensure their intentions and best interests in helping the collective society. Consequentialist, duty, and virtue are the three mindsets of the framework which define ethical conduct, focus, motivation, and the deliberative process. A duty mindset is conducted when the obligation is to do the right thing and perform the right action above all else. An individual consequentialist focuses on the outcomes produced to achieve the most good. Maintaining donor privacy is in the best interest of nonprofit benefactors, so a consequentialist would strive to execute a decision on behalf of maintaining donor privacy. In the Blackbaud hack, the best way to maintain privacy seemed to pursue the consequentialist framework by paying the ransom. Virtue involves an individual's characteristics and behavior, if this ethical framework element was implemented with the hack, the executive would embody honest transparency. However, that was not the case and the responsibility for abiding by fell on the responsibility of the nonprofits who had to consider their duty to contact donors. From an ethical framework standpoint, Blackbaud should have reported this disaster to the nonprofits, but their consequentialist behavior in keeping the hack and ransom payoff secret backfired. They hoped to retrieve the data or assure its destruction. While this was not in the best

interest of their nonprofit partners, it was in the best interest of Blackbaud, they chose to remain centric to their own mission. They thought this lack of disclosure would assist in the future to maintain their clientele, allow investigation time to pass, and retreat to uncover the crime. Unfortunately, Blackbaud was wrong. As mentioned, they discovered in September 2020 that clients used the platform in unanticipated ways which left specific data fields unencrypted. It would have been better if a virtue perspective was chosen, then the public and donors would have won, or if duty was chosen nonprofits would be centric. Instead, nonprofits were left to fend for themselves and when consulting Blackbaud they were directed to their website or public legal statement on the matter. Donor privacy was at stake and Blackbaud made poor choices selecting an unethical course of action, placing donors at risk of disclosure. In this case, all the stakeholders - Blackbaud, nonprofits, previous and current nonprofit donors, board members, and all stakeholders were in tension. Ethical conduct is important in all organizations and nonprofits come under close scrutiny in protecting the privacy of their donors. While Blackbaud made a poor decision with poor consequences, perhaps this ethical dilemma placed them on a watchlist to enforce the Analytical Framework for Ethics to better service their clients.

Donor privacy has its flaws, but so does donor disclosure. The line between transparency and privacy is often negligible. Privacy is regulated differently on state and local levels often with various IRS tax implications. Disclosure is not always obvious, in fact while it should be easy to achieve it is inhibited by factors both internal and external such as socioeconomic, cultural, and political ramifications. Most importantly, nonprofit missions play a humanitarian role in society, they provide vital health, emergency aid, food, housing, and advocacy to correct the injustices of the United States where the government often falls short to provide public assistance. Nonprofits exist for the sole purpose of helping the collective society with no

remuneration in return. So, the question exists, Donor Privacy or Disclosure: Which is Better? This is a complex choice and decision. However, to increase nonprofit impact and be mission and donor centric, nonprofits need to continually communicate with stakeholders to weigh the benefits of donor privacy versus donor disclosure. Perhaps, if nonprofit organizations partnered with public and private entities then regulations could be adopted that maintain philanthropic freedoms, as guided by America's founding fathers, while ensuring contributions are transparent and void of fraud.

References

Association of Fundraising Professionals. (1993). Donor Bill of Rights. *Association of Fundraising Professionals.* https://afpglobal.org/donor-bill-rights.

AAMC Compliance Officers' Forum Privacy Workgroup. (2014, April). When Federal Privacy Rules and Fundraising Desires Meet: An Advisory on the Use of Protected Health Information in Fundraising Communication. *Association of American Medical Colleges.* https://www.aamc.org/system/files/c/3/376966-hipaa_advisory.pdf.

BBB Wise Giving Alliance. (2003). BBB Standards for Charity Accountability. *Give.org.* https://www.give.org/charity-landing-page/bbb-standards-for-charity-accountability.

Bryan, Stuart. (2016, Dec 6). Why Nonprofit Must be Especially Capable with Their ePHI Data Security. *The Nonprofit Quarterly. https://nonprofitquarterly.org/nonprofits-must-especially-careful-ephi-data-security/.*

Charity Navigator. (2020). Donor Privacy Policy. *Charity Navigator*. https://www.charitynavigator.org/index.cfm?bay=content.view&cpid=1850#.VsOTGvkrLIU.

The Center for Public Integrity. (2020). Donor Privacy Policy. *The Center for Public Integrity.* https://publicintegrity.org/donor-privacy-policy/.

Clolery, Paul. (2020a). The Hack of Blackbaud: Damage is Still Being Accessed. *The Nonprofit Times.*https://www.thenonprofittimes.com/npt_articles/the-hack-of-blackbaud-damage-is-still-being-assessed/.

Clolery, Paul. (2020b). Some Donor Data Accessed in Blackbaud Hack. *The Nonprofit Times.* https://www.thenonprofittimes.com/npt_articles/breaking-some-donor-data-accessed-in-blackbaud-hack/.

Filla, J. & Brown H. (2013). Ethics, Risk, and Data Protection: What's the Big Deal? *In Prospect Research for Fundraisers: The Essential Handbook.* Association of Fundraising Professionals.

Florino, Joanne. (2020). Philanthropic Freedom: What It Means and Why It Matters. *Philanthropy Roundtable.* https://www.philanthropyroundtable.org/docs/default-source/default-document-library/final-edits-from-kd-ts_philanthropic-freedom--what-it-means-and-why-it-matters.pdf?sfvrsn=d2b9ae40_1.

For Purpose Law Group. (2018). Donor Privacy: Every Nonprofit Should Have One. *For Nonprofit Law Group, LLP.* https://forpurposelaw.com/donor-privacy-policy/.

Independent Sector. (2015). *Principles for Good Governance and Ethical Practice: A Guide for Charities and Foundations*. Independent Sector.

Mississippi Center for Public Policy. (2019, Mar 28). Govt. Bryan signs donor privacy law. *Mississippi Center for Public Policy*. https://mspolicy.org/mcpp-commends-gov-bryant-for-signing-donor-privacy-legislation/.

Nese, M. (2015, June 16). Three primary threats to 501(c)(3) Donor Privacy. *Institute for Free Speech.* https://www.ifs.org/research/three-primary-threats-to-501c3-donor-privacy/.

Office of the Attorney General. California Consumer Privacy Act of 2018. *State of California Department of Justice.* https://oag.ca.gov/privacy/ccpa.

Office of Civil Rights. (2003, May). Summary of HIPAA Privacy Rule. *United States Department of Health and Human Services.* https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

Parnell, Sean. (2017). The Legal and Political Landscape of Donor Privacy. *Philanthropy Roundtable.* https://www.philanthropyroundtable.org/philanthropy-magazine/article/spring-2017-the-legal-and-political-landscape-of-donor-privacy.

Philanthropy Roundtable. (2017, June 22). *Philanthropy Roundtable.* https://www.philanthropyroundtable.org/docs/default-source/default-document-library/protecting-philanthropic-privacy_white_paper.pdf.

Philanthropy Roundtable. (2020). Donor Privacy: Expanded Protections, Growing Threats in 2020. *Philanthropy Roundtable.* https://www.philanthropyroundtable.org/docs/default-source/default-document-library/final_donorprivacyreport.pdf?sfvrsn=2255ae40_1.

Scanlan, Eugene A. (2013). Public Privacy: An Exploration of Issues of Privacy and Fundraising. In J. Pettey (Ed.), *Nonprofit Fundraising Strategy: A Guide to Ethical Decision Making and Regulation for Nonprofit Organizations*. (2nd ed., pp. 53-77). Hoboken: John Wiley & Sons.

Schroeder, T. (2016), Respect and Honor Donor Privacy. *The Major Gifts Report*, *18*, 8. https://doi-org.ezproxy.cul.columbia.edu/10.1002/mgr.30509.