NAVIGATING THE DATA PRIVACY MAZE:
A Guide for Nonprofits

Bruce Hammer, Path2Response

In today's digital age, data is the lifeblood of nonprofit organizations. It fuels fundraising efforts, personalizes donor communications, and drives impactful campaigns. As nonprofits gather more information about their supporters, they must be increasingly mindful of their ethical and legal responsibilities when handling that data.

In addition, the ever-evolving landscape of state-level privacy laws presents nonprofits with a daunting challenge: staying compliant while effectively leveraging data to advance their missions. Most states have comprehensive privacy laws that exempt nonprofits, but a few notable states do not. It's important to look up the privacy regulations in your state to ensure your program is compliant.

The Stakes Are High

Data privacy is not just a legal requirement; it's a matter of trust. Donors entrust us with their personal information, and it's our responsibility to safeguard it. A data breach or misuse of information can harm consumers, severely damage an organization's reputation, and erode donor confidence.

Navigating the Privacy Landscape

Here are some key considerations for nonprofits navigating the data privacy maze:

1. UNDERSTAND THE LAWS:

Familiarize yourself with relevant privacy laws, including:

- GDPR (General Data Protection Regulation): While a European Union law, GDPR has global implications and sets a high standard for data protection.

- CCPA (California Consumer Privacy Act): A landmark U.S. privacy law with strict requirements for businesses handling California residents' data.

- State-specific laws: As of this writing, nineteen states have enacted comprehensive privacy laws, each with unique provisions. Thirteen of these exempt nonprofits, while six do not.

2. IMPLEMENT DATA PROTECTION MEASURES:

- **Know your data:** Create a comprehensive inventory of all the data you collect—document where it's stored, how you use it, and who can access it.

- **Data security:** Implement robust security measures to protect data from unauthorized access, use, or disclosure.

- **Data minimization:** Collect only the data you need for your specific purposes.

- **Transparency:** Be transparent with donors about collecting, using, and protecting their data.

3. PRIORITIZE CONSENT AND CHOICE:

- **Obtain consent:** Obtain explicit consent from donors before collecting or using their data.

- **Provide choice:** Give donors choices about how their data is used, including opting out of marketing communications.

- **Respect preferences:** Honor donor preferences regarding data sharing and communication frequency.

4. BUILD A CULTURE OF PRIVACY:

- **Training:** Train staff and volunteers on data privacy best practices.

- **Data governance:** Establish clear policies and procedures for data handling and access.

- **Regular audits:** Conduct regular audits to ensure compliance with privacy laws and internal policies.

TIPS AND STRATEGIES FOR SUCCESS:

- **Stay informed:** Keep up-to-date on the latest privacy laws and regulations.

- **Support and engage:** Learn from and support organizations like the International Association of Privacy Professionals and the Future of Privacy Forum.

- **Seek expert advice:** Consult with legal counsel or privacy professionals to ensure compliance.

- **Embrace technology:** Where applicable, leverage technology solutions to automate data privacy processes and enhance data security.

- **Communicate clearly:** Communicate your commitment to data privacy to your donors and stakeholders.

The Path Forward

Navigating the data privacy landscape is an ongoing journey, not a destination. By prioritizing ethical data handling, staying informed, and implementing robust safeguards, nonprofits can build trust with their supporters and ensure compliance. Remember, data privacy is not just about protecting information; it's about empowering your mission.

Message *from the* President

Dear friends and fellow DMFA members,

The first few months of 2025 have brought a great deal of uncertainty for many nonprofit organizations and their marketing partners. During these turbulent times for our industry, please know that you are not alone. The DMFA is here to support our members and offer guidance through our education and programming, and will continue to share information from industry partners to help navigate these unforeseen challenges.

This newsletter takes you on a deep dive into data privacy, an issue that continues to take on greater importance in our field. We have several articles devoted to the topic, but I wanted to draw your attention to page 12 that provides a summary of the DMFA's February 11 webinar, *The Evolving Landscape of Data Privacy Legislation: What Nonprofits Need to Know.*

The webinar featured Britt Vatne, President of Adstra (and former DMFA President), and Shannon McCracken, CEO of The Nonprofit Alliance. It was an invaluable conversation about the current data privacy environment. The enclosed article provides some of the highlights of this conversation, including 5 key steps for nonprofits to take to ensure they are in compliance with existing laws and appropriately protecting their donors.

In addition to the chance to brush up on your data privacy knowledge, this issue of the newsletter helps you get to know the winners of our 2024 Marketer of the Year and Spark awards, and selected Organization of the Year. We announced and introduced you to these industry leaders in December's issue and were able to honor them at our wonderful year-end event on December 5th. It's a pleasure to be able to more fully share their stories with you here. I hope you are inspired by their achievements and contributions to our industry.

Spring is a busy time of year, which is especially true at the DMFA. We have several exciting events coming up in the next few months that I hope you'll choose to work into your busy schedule:

- DC Networking Happy Hour— Monday, April 28
- Spring Sustainer Group Meeting— Tuesday, May 13

  INAUGURAL EVENT!

- 2025 DMFA Awards Celebration and Annual Membership Meeting— Thursday, June 5

It's clear that 2025 could be tumultuous for our industry. Amidst these uncertainties, I hope you find solace in knowing that the DMFA will continue to serve as a resource while we navigate these challenges together. Thank you for your continued involvement. I hope to see you at an upcoming event.

Best,

Kristen Shank Finn

Kristen Shank Finn
President, DMFA

Privacy Revealed: Is it really that big of a deal?

Michael G. Solomon, PhD, Production Solutions

> **How can we protect data from disclosure AND keep an individual's identity private?**

One of the hottest terms to in today's conversations about data is "privacy." Many people call it "data privacy," but that phrase confuses the issue. For several decades technical specialists have struggled with the best ways to secure data. As the internet grew and supported the World Wide Web to make accessing data and resources easy regardless of location, so did concerns over security. Making something easy to access makes it an attractive target for malicious players. Thus, information security matured to protect data.

CIA—The Golden Triad

The field of information security defines three primary tenets, each of which is required to ensure the security of any information:

- **Confidentiality:** Only authorized entities are allowed to access data

- **Integrity:** Only authorized entities are allowed to modify data

- **Availability:** Information is accessible on demand by authorized entities

There are other tenets that have been added over the years, but the "big three" cover the foundational needs of security.

In the context of privacy, many people equate confidentiality with privacy. That is not only technically inaccurate, but also very misleading. Before we get to a clearer definition of privacy, let's look a bit more closely at confidentiality.

The most common methods used to enforce confidentiality are access controls and encryption. Access controls used to be the go-to choice to protect data when that data conveniently resided in internal databases. As distributed systems and cloud computing have become the standard, data routinely travels across the internet to many points of use. In many cases, there is no single trusted authority to manage who accesses data. In the absence of a central entity, encryption can step in to help. The only users who can decrypt user data are those who hold the keys to decrypt the data. Although encryption adds complexity to processing data, it can help to ensure that only authorized entities can access data.

To keep things moving forward, I am going to gloss over a few technical details. Researchers are investigating several new types of encryption that simplify the difficulties of managing keys. If you are interested, take a look at research into functional encryption techniques and quantum cryptography.

Privacy

Privacy differs from confidentiality in that what each one protects is different. Confidentiality focuses on data. If you control who can access data, you can assure its confidentiality. Conversely, privacy's focus is on the individual. While data may represent the attributes of an individual, associating an individual's identity with data discloses that identity and violates their privacy.

The main question for protecting confidentiality and privacy in operations is: How can we protect data from disclosure AND keep an individual's identity private? This question consists of two radically different challenges.

One of the amusing discussions in security and privacy circles is the conflict between repudiation and nonrepudiation. Nonrepudiation means that every action is associated with an identity. In other words, we need nonrepudiation to log who did what and when. We use that information to make decisions on whether to grant or block access to data and resources and to trace the provenance of data. However, if every action can be traced to a unique individual, that individual's privacy is sacrificed. To detach action from identities (e.g. do not record that a specific person takes medication for a certain degenerative condition), we must reject nonrepudiation and enforce repudiation. Digging into this tension is beyond the scope of this article, but it serves to point out that privacy is far more than just enforcing confidentiality.

Organizations that handle sensitive data (any data that can be used to identify a unique individual) must deploy controls to protect the privacy of individuals. Far too many organizations deploy confidentiality controls and just stop there. While turning on encryption may satisfy some of the weaker compliance requirements, that action alone does little to protect privacy.

The first step toward protecting an individual's privacy is to identify sensitive data. Any data that can be used to identify an individual is sensitive data. That can include the obvious attributes such as name, address, gender, age, and ID number, as well as less obvious data that may include education, donation history, job function, and hobbies.

If you doubt that hobbies are considered sensitive data, I will give you a challenge to figure out my age. Assume that you see on a social media post that I am a runner. If you also knew the general location where I live, you would find that there is a large road race that attracts many runners, year after year. A quick search of past race results would return my name and reveal my age on race day. That is an example of privacy disclosure through

data triangulation. Protecting individuals' privacy means denying malicious actors the data that they can use in triangulation.

Once you identify sensitive data, the real work starts. The key to ensuring privacy is to disassociate all data you release from individuals. For individual records (e.g. an individual's descriptive data), careful use of confidentiality controls will do the trick. However, data in reports, exports, and dashboards can inadvertently violate privacy. It is important to examine the meaning of data that you release, not just its format or content. Access to donation history can indicate a person's financial status and beliefs. If you publish a report or export data that is detailed enough to allow its readers to infer an individual's identity, you are not protecting that person's privacy. In such cases, one approach would be to alter the output to either obfuscate or aggregate data. Privacy controls can be complex and often go far beyond the minimums of current privacy requirements.

Privacy is not a new concern. Once the problem gained initial attention, early efforts to ensure privacy were based on anonymizing common identifiers. Unfortunately, it quickly became evident that such approaches were insufficient. It is easy to find several notorious examples that highlight the weaknesses of anonymization.

Anonymization Is Not Good Enough

Two early examples of the weakness of anonymized data point out that simple solutions are not always the best solutions. Privacy researchers uncovered ways to pierce the false protection that anonymization was supposed to provide and figured out how to re-identify subjects. While these examples may seem to be dated, remember that both outcomes resulted from old-fashioned research before many of today's advanced tools (including AI) emerged.

Massachusetts Group Insurance Commission

In 1997, the Massachusetts Group Insurance Commission (GIC) released anonymized state employee data that included details of individual hospital visits. The reason they did this was to promote research into improving the quality of health care while reducing cost.

Latanya Sweeney, an MIT computer science Ph.D. student at the time, used the GIC data to conduct successful re-identification research. Dr. Sweeney purchased voting records for Cambridge, Mass., for $20 and used that data, along with the GIC data, to uniquely identify hospital visits by the Massachusetts governor at the time, William Weld.

Dr. Sweeney published a seminal paper in 2000 in which she documented that 87 percent of all Americans could be identified with only their ZIP code, gender, and date of birth. Dr. Sweeney's research demonstrated that privacy is a difficult problem because so little data is needed to identify individuals.

AOL Search Data

In August 2006, AOL released "cleansed" logs containing 20 million search queries for over 650,000 users. The data was released as part of a competition to increase search engine accuracy. The data directly identifying individual users had been anonymized, and AOL personnel assumed associating users with the queries they submitted was not possible.

Investigative reporters with *The New York Times* also looked at the data and wondered what they could learn from it. After analyzing the search queries, they found that user 4417749 searched for some interesting things, including:

- "landscapers in Lilburn, Ga"
- Several people with the last name Arnold
- "homes sold in shadow lake subdivision gwinnett county georgia"

The reporters used these searches, along with others from the same user, to determine that user 4417749 was actually Thelma Arnold, who lived in Georgia. They contacted her and she confirmed that the queries were hers.

### Online Privacy—Where Do We Go from Here?

The moral of this story is that well-intentioned controls to protect privacy often fall short. The only way to protect privacy is for organizations that collect and handle personal data to do so responsibly. Clearly, that is easier said than done.

Sensitive data can be used to uniquely identify an individual and therefore has great value to businesses. Sensitive data allows organizations of all types to target their marketing efforts, and because of this inherent value of such data, many organizations have been collecting private data for decades.

Collecting, and often misusing, sensitive data has gotten the attention of legislators across the globe. Governing bodies from many nations are incorporating privacy concerns into regulation and legislation. Arguably the most comprehensive effort to date is the European Union's General Data Protection Regulation (GDPR). The GDPR goes far beyond any previous efforts to protect individual online privacy. Among other things, it requires that all EU citizens be given clear notification of what personal data is being collected and stored, how it will be managed, and how it will be used. The GDPR also requires that users be able to request that all their private data be deleted upon demand.

Although the EU ushered in the privacy awareness revolution, an increasing number of countries and U.S. states are following suit. The GDPR has already disrupted the way organizations conduct business online, and online data privacy is now in the global spotlight. This groundbreaking regulation may have made some things difficult for online business, but it is a great step forward for consumers.

As we see online activity and data collection maturing, it is important for all users to pay attention to the data you're giving away. Your data tells your life's story. Pay attention and choose wisely. ***Your privacy is valuable and worth protecting.***
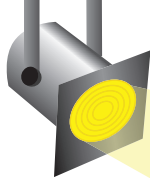
MEMBER ORGANIZATION
SPOTLIGHT

CENTER *for* REPRODUCTIVE RIGHTS

Every year, the DMFA recognizes a nonprofit organization whose programmatic work and business practice reflect the spirit of our Diversity, Inclusion, and Systemic Change (DISC) pledge. This past December, at our year-end event in NYC, we named the **Center for Reproductive Rights** as our Organization of the Year.

The Center for Reproductive Rights is a global human rights organization of attorneys and advocates working to ensure reproductive rights are protected in law as fundamental human rights for the dignity, equality, health, and well-being of every person.

Since its founding in 1992, the Center's game-changing litigation, legal policy, and advocacy work—combined with unparalleled expertise in constitutional, international, and comparative human rights law—has transformed how reproductive rights are understood by courts, governments, and human rights bodies. Because of the Center's work, over the past two years, 2.3 billion more people are living under stronger legal protections for reproductive rights. In addition, the Center has:

- Won groundbreaking cases before national courts, UN committees, and regional human rights bodies.
- Participated in every major U.S. Supreme Court abortion case since its founding.
- Strengthened reproductive laws and policies in over 65 countries across five continents.

The Center for Reproductive Rights is wholly committed to fostering a diverse, equitable, and inclusive organization. Its board embraces the Center's DEI commitments and its plans for more fully realizing them in the Center's programmatic work and its workplace.

MARKETER of the Year

From Knocking on Doors to Knocking Out Fundraising Goals:

A Conversation with Karin Kirchoff, Marketer of the Year

The Marketer of the Year Award recognizes a DMFA member for their extraordinary achievements and contributions to the direct marketing field. In 2024, we honored **Karin Kirchoff, president and founder of K2D Strategies**.

We recently sat down with Karin to talk about her 30-year career in direct response—a career that started in the political arena. After graduating from college, she volunteered for the DNC ahead of the 1992 presidential election and soon found herself knocking on doors. Ultimately, she worked for three different candidates and lived in seven separate states.

Her passion for grassroots politics and love for crafting compelling arguments led her to fundraising for a telemarketing firm. From there, she transitioned to working directly with nonprofits, running the mid-level program at the Human Rights Campaign, raising $25 million per year as the vice president of membership for Defenders of Wildlife, and serving as deputy executive director at National PTA.

Karin also found time in her busy career to cut her teeth at two separate direct marketing agencies, where she developed a deep appreciation for the role data plays in campaign targeting, offer development, and retention strategies. In the weeks following the 2016 election, she founded the agency K2D Strategies to directly serve nonprofits actively changing the world.

When asked what advice she would give someone early in their career who wants to move up in direct marketing, she responds immediately: "Make meaningful connections. Ask questions. Own your own mistakes, and don't be afraid to fail. If you're not failing at something, you're not learning."

In addition, Karin recommends never turning down an opportunity to get involved in our industry, and notes that her first-ever industry presentation was at a DMFA lunch-and-learn session on lapsed reinstatement strategies. "Volunteering has been hugely impactful on my career development, and the DMFA was always accessible, friendly, and made it easy to get involved."

Turning reflective, she notes that she's been a Girl Scout since the age of six, which taught her the important lesson of leaving a place better than you found it. "I carry that forward in my life today. I want our world to be a better place—to be kinder, happier, more welcoming. And I want this amazing industry that I have the tremendous privilege to be a part of to be better today than it was yesterday."

From all of us at the DMFA, we congratulate Karin as our Marketer of the Year—and we thank her for helping us shape this industry for the better.

DMFA Spark✦Award

Celebrating the Next Generation of Leaders:
Meet Katie Tamaro, Spark Award Winner

CITYMEALS ON WHEELS

The **DMFA Spark Award** was launched in 2024 and recognizes emerging leaders in the world of direct marketing fundraising who have made significant contributions through innovative projects or volunteer work.

We're thrilled to introduce you to Katie Tamaro, our inaugural Spark Award winner!

After beginning her career at Integral and Lautman Maska Neill & Company, she joined Citymeals on Wheels in 2024. As their digital fundraising manager, she leverages her expertise to elevate digital campaigns and drive impactful results—all to support the organization's mission to provide meals and vital connection for homebound elderly New Yorkers.

Katie's passion for helping others is what drew her to this industry, and what keeps her going. She says, "Fundraising is more than just work. It's about creating tangible change and being a part of something bigger than yourself."

When asked what advice she would give to someone just starting out in the field, she recommends an open mind, hunger to learn, and a healthy respect for the old-school strategies that have stood the test of time. She also notes, "Our industry is rich with opportunities for professional development, so take advantage of every chance to grow. Find a mentor or someone you admire, and don't hesitate to learn as much as you can from them."

As for her own mentors, she names Rachel Penney, Kate Hollandsworth, Rachel Kottler, and her current director, Andrea C. Weyhing. She says, "Each of these women has mentored me at different points in my journey, and their guidance has been invaluable. I wouldn't be where I am today without their support, and I'm deeply grateful."

Katie also cites professional organizations like the DMFA as an important factor in her own development as a fundraiser. She says, "The DMFA has been a fantastic resource. Their educational events have provided valuable learning opportunities, and the networking aspect has been incredibly beneficial. I've been able to connect with industry peers, exchange ideas, and build connections."

Describing her reaction to finding out that she had won the DMFA Spark Award, Katie says, "I was so thrilled that I ran straight into my director's office to share the good news, and we couldn't help but celebrate! Winning the Spark Award was an incredibly exciting and humbling moment for me. I've always admired so many inspiring individuals in this industry, so being recognized among them is such an honor."

From all of us at the DMFA, we're honored to count Katie as part of our community of committed fundraisers. Congratulations again!

If you know an emerging leader with less than five years of experience in the field of direct response fundraising (whether starting their careers or transitioning from another sector), please keep them in mind for the 2025 DMFA Spark Award. Nominations will be collected in Fall 2025.

PROTECTING DONOR TRUST:
The top cybersecurity measures every nonprofit should take

Kim Abuelhaj, GLAAD

Cybersecurity is crucial for nonprofits, especially when handling donor data. Here are the top cybersecurity measures every nonprofit should take to ensure your data, privacy, and security is protected:

- **Implement Strong Password Policies**—Require long, complex passwords and enable multi-factor authentication (MFA) for all accounts. Use a secure password bank to safely store credentials and prevent breaches from weak or reused passwords.

- **Keep Software and Systems Updated**—Regularly update operating systems, software, and plugins to patch vulnerabilities, and establish a process to ensure organization-wide compliance.

- **Use Encrypted Communications**—Encrypt emails and sensitive files to prevent unauthorized access. Quarantine incoming emails to detect and block threats like spam, phishing, and malware before they reach staff.

- **Conduct Regular Security Training**—Implement a training solution like NINJIO to provide ongoing, engaging security awareness trainings to keep staff educated about phishing and safe online practices.

- **Limit Access and Permissions**—Give people access only to the information and tools they need to do their job, and nothing more. This helps minimize risks and protect sensitive data from unauthorized access.

- **Secure Donor and Financial Data**—Use encrypted databases, implement external scanning services to demonstrate PCI DSS compliance, and ensure adherence to data protection laws like GDPR or CCPA to maintain payment data security.

- **Implement Firewalls and Endpoint Protection**—Deploy strong firewalls, antivirus software, and endpoint detection to prevent malware attacks.

- **Regularly Back Up Data**—Regularly back up your data in a secure, offsite environment to protect against data loss from potential ransomware or system failures.

- **Develop an Incident Response Plan**—Have a clear plan for responding to security breaches, including communication strategies. Encourage staff to report attacks immediately for swift action.

VOICES FROM OUR INDUSTRY:
Data Privacy Challenges and Recommendations

"Data privacy is a core issue for the ACLU so our policies are centered around maintaining and expanding our donors' right to privacy. To that end, we're consistently tweaking and updating policies. But as fundraisers, we do need access to data to be efficient, so we also know it's important to build trust with donors around how we use their data by being as transparent as possible. We go above and beyond to make sure our privacy policy is clear to donors and that we adhere to it. And if there are data issues, reaching out immediately to let them know."

—Nosa Adetiba, America Civil Liberties Union (ACLU)

"Respecting donors' wishes about their data is paramount for nonprofits of all sizes—not only for compliance reasons, but also to foster a sense of trust with valued supporters. Nonprofits should have clear policies in place for how data is stored and transmitted, who has access, and how specific data can and cannot be used. Having written policies is just the first step; you also need to ensure that the people tasked with responding to queries are prepared and comfortable discussing these issues when donors reach out to ask."

—Lisa Maska, CFRE, Lautman Maska Neill & Company

"Nineteen states have passed data privacy laws, and seven specifically cover nonprofits. Although there are many similarities among these laws, they require organizations to ensure they are compliant on a state-by-state basis. This patchwork approach is burdensome for a nonprofit, increasing costs and potentially limiting innovation, while also running the risk of confusing the donor. There is a real need to have one comprehensive data privacy law that pre-empts the individual state laws. The TNPA has been a strong advocate, bringing nonprofits and their commercial partners together to lobby legislators."

—Britt Vatne, Adstra

"Many of the common practices fundraisers use to reach new donors or learn more about prospects are invasive of people's privacy. We know this at a gut level but convince ourselves that they are necessary evils. They aren't. They cause privacy harms to the people we are fundraising from and create relationships with trust already in need of repair."

—Allison Morris, Electronic Frontier Foundation

"Every donor who makes a gift to a nonprofit organization has two basic assumptions. First, that the gift will be used as promised. Second, that the donor will not harmed because of their gift. Having strong data privacy protections in place is a critical way to ensure that nonprofits honor that implicit promise."

—Rich Kostro, Share Our Strength | No Kid Hungry

"In 2025 where nonprofits are just as much a data company as their commercial counterparts, having a data privacy policy is critical. Staying up to date on data privacy regulations and current concerns is necessary, especially when guarding your donor data, which is one of the most valuable assets you have."

—Ryan Carpenter, Allegiance Group + Pursuant

"It's important to be proactive on issues of data privacy. Nonprofits can take a 'privacy-first' approach to the management of donor data by implementing industry-leading standards of care. This can be accomplished in-house with a privacy compliance officer working in tandem with outside counsel and/or professional privacy resources such as the IAPP."

—Bruce Hammer, Path2Response

The Evolving Landscape of Data Privacy Legislation:
What Nonprofits Need to Know

This article summarizes information shared in DMFA's February 11 webinar with Britt Vatne, President of Adstra, and Shannon McCracken, CEO of The Nonprofit Alliance.

The data privacy regulatory environment continues to expand rapidly across the United States, creating new challenges and considerations for nonprofit organizations and their partners. As of early 2025, 19 states have enacted consumer data protection laws, with seven specifically covering nonprofit organizations. This marks a significant increase from just 13 states with such laws a year ago, highlighting the accelerating pace of privacy legislation.

While many state laws exempt nonprofits from direct regulation, organizations shouldn't assume they're unaffected by these laws. Most nonprofits rely on commercial partners and data brokers subject to these regulations, meaning the ripple effects—including reduced data availability and higher costs—impact the entire sector. Colorado, Delaware, Indiana, Maryland, Minnesota, New Jersey, and Oregon are the seven states currently including nonprofits in their privacy legislation.

Core Components of Current Legislation

Despite variations between states, most privacy laws share common fundamental elements. They typically provide consumers with several key rights:

— The right to know what personal information is being collected and how it's used

— The right to delete personal information

— The right to opt out of data sharing

— The right to correct inaccurate personal information

Additionally, some states have implemented data minimization requirements, limiting collection to information that is directly relevant and necessary for specific purposes. There's also growing attention to "sensitive data" categories, though the definition varies by state. Many data providers are already restricting the use of religious and ethnic data in response to these concerns.

Impact on Nonprofit Operations

The practical effects of this legislative wave are being felt across the nonprofit sector. Due to privacy concerns, many commercial data sources have ceased renting or exchanging their data assets. This includes valuable prospect audiences that nonprofits have historically relied upon for direct mail fundraising, such as current check buyers. The combined impact has been substantial—large sources of data used by nonprofits have declined 35% over the past three years.

Looking Ahead: Federal Legislation and State Trends

While state-level activity continues to expand, the prospect of federal privacy legislation remains uncertain. Previous attempts, including the American Data Privacy & Protection Act considered in the last Congress, failed to advance due to fundamental flaws, including multiple carveouts for existing state laws and the inclusion of a private right of action that could encourage frivolous lawsuits. A Republican Senate could, on this issue, work

in nonprofits' favor; Majority Leader Thune (R-SD), Commerce Committee Chair Sen. Cruz (R-TX), and Commerce Committee member Sen. Moran (R-KS) are in key positions and have a long history of advocating for national privacy legislation to preempt state statutes. We will, however, need support from at least seven Democrats to break a nearly certain filibuster. Comprehensive data privacy legislation could move faster on the House side, where only a simple majority is necessary to pass a bill.

Oklahoma again emerged as a significant state to watch in 2025, with two competing privacy bills under consideration. One proposal would implement the nation's first opt-in requirement for data collection, while a competing bill follows the more common opt-out model. The outcome could set an important precedent for other states considering similar legislation. Oklahoma attempted to pass an opt-in bill twice before, and while those were not successful, there is no guarantee that a third attempt will similarly fail.

New York is also worth watching. In 2024, proposed legislation would have covered both nonprofits and commercial entities. The Assembly and Senate couldn't reconcile differences, but the legislation was reintroduced in both chambers in 2025.

California continues to lead the way in expanding privacy protections. The California Delete Act, set to take effect in January 2026, will provide consumers with a streamlined process to request data deletion across all registered data brokers. The state has also broadened its definition of data brokers to include organizations that sell personal information they didn't collect directly from consumers.

Action Items for Nonprofits

Given this complex and evolving landscape, nonprofits should take several key steps to ensure compliance and protect donor relationships:

1. Regularly audit and update privacy policies, particularly regarding digital practices

2. Develop clear protocols for responding to donor privacy requests, regardless of whether your organization is legally exempt

3. Implement strong data governance and security practices, including multi-factor authentication and employee training

4. Practice data minimization, collecting and retaining only the data needed for specific purposes

5. Maintain easily accessible opt-out mechanisms and clear information about data use

The Path Forward

As privacy legislation continues to evolve, nonprofits must stay informed and adaptable. While the current patchwork of state laws creates compliance challenges, it also presents an opportunity for organizations to demonstrate their commitment to donor privacy and build trust with supporters. By taking a proactive approach to data privacy and maintaining transparent practices, nonprofits can navigate this changing landscape while maintaining effective fundraising and donor engagement programs.

Organizations should continue monitoring legislative developments, particularly in states where new bills are under consideration. Working with data partners to understand their compliance measures and any resulting changes in data availability will also be crucial for maintaining successful fundraising programs in this new environment.

For more information and up-to-date legislation summaries, visit **https://tnpa.org/get-involved/privacy/**.

Have a question or need fundraising advice? Connect with your industry peers on the DMFA Forum!

Recent threads include:

- CRM recommendations
- Mid-year budget reforecasting
- DAF providers and financial advisors
- Year-End email subject lines
- Cultivations that raise funds

DMFA members can access our dedicated discussions board by logging in at **dmfa.org** and navigating to **Forum** on the lefthand menu.

DMFA
Professional Development Fund

The DMFA believes that when any one of us becomes a better fundraiser, it helps lift up our peers as well. That's why the DMFA Professional Development Fund was created—to help fundraisers, and those interested in fundraising as a career, pursue education by subsidizing some of their costs. This scholarship is available to nonprofit organizations, students, and non-working professionals.

If you fit into one of the above categories and want to further your career with a conference, webinar, or membership, apply here:

https://dmfa.org/awards/prof-dev-fund/
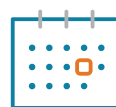
Save the Date

APRIL

- **DC Networking Happy Hour**
  04/28/25, 5:00 PM – 7:00 PM (EDT)
  LOCATION: Roofers Union 2446 18th Street NW, Washington, DC

- **2025 Mid-Level Giving Benchmarking Summit**
  04/29/25, 8:00 AM – 7:00 PM (EST)
  04/30/25, 8:30 AM – 2:30 PM (EST)
  LOCATION: College Park Marriott Hotel and Conference Center, 3501 University Blvd East, Hyattsville, MD

MAY

- **Spring Sustainer Group Meeting**
  05/13/25, 3:00 PM – 5:00 PM (EDT)
  LOCATION: Zoom
  Invite Only

JUNE

- **2025 DMFA Awards Celebration and Annual Membership Meeting**
  06/05/25, 11:30 AM – 4:30 PM (EDT)
  LOCATION: Royalton Park Avenue, 420 Park Avenue South (at 29th Street), New York, NY

- **DC Lunch: Diversifying Your Donors**
  06/12/25, 12:00 AM – 3:00 PM (EDT)
  LOCATION: The Gathering Spot 1720 I Street NW Washington DC
  SPEAKERS:
  Iván León, *Chief Strategist,* **Kerux Group Inc.**;
  Jodie L Ruediger, *CFRE, Associate Director, Collaborative Direct Marketing,* **Habitat for Humanity**

Be sure to check your email and dmfa.org for more information.

Midlevel Giving Spotlight

How Mid-Level Programs Use Surveys to Both Inform and Engage

Jeff Muller, Crossroads Insights LLC

As the experiences of numerous fundraising programs has demonstrated, surveys can be powerful tools for growing and nurturing mid-level audiences. On the one hand, they can be a method to engage a large, geographically distributed audience, providing a platform to create virtual dialogue at scale. On the other, they can uncover key insights that help better communicate with and steward this important community of donors that so often provides an essential pool of unrestricted funds. How that data is handled and whether donors are kept anonymous depends on the project and desired results.

In late February, as everyone was getting excited about the 2025 DMFA Mid-Level Giving Benchmarking Summit coming up at the end of April, I spoke with three mid-level experts—A.J. Minogue from Orbis, Megan Den Herder from the Wildlife Conservation Society (WCS), and Barbara Camick from Best Friends Animal Society—about how mid-level shops can think about deploying surveys to advance their programs. Here are the key takeaways from that conversation:

First Determine Your Survey Goals

Informed by his years of experience with data analytics, A.J. encourages a pragmatic approach to kicking off any survey effort. "There's a decision tree moment when you determine what the survey is going to be." He suggests first establishing the primary goal of the survey. In particular, it is important to determine if the survey is needed to gather market research or if it is being used as a method of donor engagement. That decision will inform the best approach to data collection and what kind of data will be available.

According to A.J., "if you're genuinely looking to gather insights about how your market group thinks about you and the work you're doing, or the work you should be doing, then being totally anonymous is the way to do it because it promotes free expression." He points out that most online survey tools provide simple ways to anonymize the data, even when directing traffic from an email or website. However, A.J. says that using SMS for surveys makes it harder to divorce the data from a person's phone number, which can sometimes interrupt the anonymity of the effort.

On the other hand, he says that using surveys as an engagement tool can be quite effective. "Filling out a survey is a nice, super engagement point and people who fill out

surveys often do it again." A.J. advises that, if your value proposition to the donor is that they know they're being heard, then it is essential to determine how much data you want to collect, what you're going to do with that information, and how you're going to share it back.

Asking the Right Questions Matters

At WCS, Megan began surveying the organization's mid-level donors when she first started five years ago, having successfully deployed the tool in previous roles at both Audubon and The Nature Conservancy. Her first piece of advice is to identify a strong partner who can help create an effective survey (she uses Sea Change Strategies). "Putting together a survey is not necessarily hard but putting together one that gets people to open up to you and really think about what they're answering is incredibly difficult."

One unique challenge that Megan faces is the dual nature of WCS's value proposition. Most of her long-time mid-level donors came to the organization through their nationally recognized New York zoos, especially the Bronx Zoo. But she has done a lot of work in her time there, and now two-thirds of her mid-level donor file support the global conservation efforts of WCS, which is also one of the largest environmental organizations in the world. According to Megan, "We've changed the shape of the file a lot, turned it less transactional and made it much more philanthropic focused. In the five years I've been here, we've been trying to figure out the right balance in our messaging. So, we've done a lot of surveys on that front."

She has also used surveys as a tool to help educate WCS's donors. "We work in over 55 countries and have thousands of field staff working to protect wildlife and wild places. But a lot of donors, especially our long-time ones, don't know that because they think of us mainly as the Bronx Zoo. So, we try to make sure our donors understand what they're donating to by sharing our impacts and the work we're doing through those surveys."

Strategically Make Use of Multiple Types of Surveys

Barbara's team at Best Friends recently surveyed the more than 8,000 members of their mid-level society, the Golden Circle, to better understand the individual preferences of their donors. While the survey results broadly reinforced that, as

a group, these donors value personalized experiences and access over tangible benefits, the data has a more targeted purpose. It will be used to inform customized communication strategies that better align with each donor's individual preferences.

Describing the initiative, Barbara said, "We asked a dozen questions about our donors' Golden Circle experience. The data has been recorded on the donor records, so if they're in a portfolio, the relationship manager already has access to the donor's responses and can act on them. Our next step is to come up with some modifications to our plan steps, so that—at scale—we're making communications adjustments based on each person's feedback." This will entail ensuring donors get the amount and type of information, and level of personalization, that best fits their preferences. According to Barbara, "Our hope is that we see an increase in donor value and commitment to the organization over time."

In addition to the Golden Circle survey, the Best Friends team conducts a monthly insight panel survey that goes to a cross section of the organization's donors, including those in the mid-level group. Each January, between 1,000 and 2,000 donors are recruited to participate over the course of the year. "We're on our fifth year of cohort groups right now," said Barbara, "so lots of great participation. One of the things we gauge is the Net Promoter Score, which is the percentage of people who would recommend the organization to friends and family. That score is always off the charts for us, and we love that our supporters are so loyal and excited to be advocates for the animals."

Interested in Learning More About Surveys to Level Up Your Mid-Level Program?

Join A.J., Megan, Barbara, and dozens of other colleagues from the more than 40 organizations that will be participating in the DMFA MLG Benchmarking Summit this April 29-30, 2025 in Hyattsville, MD. Attend general sessions for insights and analysis on your self-reported data, dive into deep discussions with your peers in focused breakout groups, and spend quality time meeting and networking with other nonprofit mid-level professionals. To learn more about this one-of-a-kind event and make your plan to attend in 2025, visit **dmfa.org/mlgbenchmarking**.