Three Critical Privacy Issues Every Nonprofit Entity Should Consider

By Deanna Coffman, GSEC, CIPP/US, CIPP/E, CIPM, FIP

This article originally appeared in BDO USA, LLP's "Nonprofit Standard" newsletter (Summer 2017).

Most nonprofit organizations collect, use and store "personal information" of donors and staff. There are well over 200 laws, just in the United States, that mandate protections of this information and apply, in whole or in part, to nonprofits. All nonprofit entities should understand the requirements that TCPA, GDPR and U.S. state data breach/protection laws impose upon their organizations.

Just a few years ago, many entities were largely unaware of the impact data privacy and cybersecurity could have on their organization overall. Most categorized these issues as belonging to the IT or HR departments. Now, data-privacy class-action litigation has erupted and data breach announcements dominate the headlines. Currently, in almost every survey conducted of boards and senior management, data issues rank as one of their three top concerns, if not their single greatest concern. Nonprofit entities would be well advised to tend to this important area which is often overlooked until it becomes a crisis.

TCPA

The Telephone Consumer Protection Act of 1991 (TCPA) was introduced in response to consumer sentiment toward unwanted telephone solicitations. Telemarketers calling during all hours—particularly the dinner hour—became a punchline and an irritant. TCPA has been updated several times over the years, and the most recent update tightens restrictions on calling without written permission, even if a "prior business relationship" existed. Nonprofit organizations are exempt from some, but not all, requirements under TCPA. For example, the "abandonment rules" are an exemption for nonprofits, and requirements for auto-dialers and prerecorded calls are different for nonprofit organizations than for commercial entities. While the requirements are less restrictive, nonprofit organizations still can't afford to completely ignore TCPA, because some requirements do still apply, and the cost for getting this incorrect can be enormous.

The recent changes give the TCPA "teeth" by providing for a private right of action, effectively inviting consumers, the FCC and states' attorneys general to join in enforcement efforts. Plaintiffs are able to recover the higher of their actual loss or $500 for each violation. And, if the court finds that the defendant acted willfully or knowingly, the court has discretion to triple the amount to $1,500 for each violation.

Organizations that conduct telemarketing should be tuned to recent changes in the TCPA. Professional plaintiffs are causing a rise in TCPA enforcement and there have been no shortage of multimillion dollar settlements. Interline Brands agreed to pay $40 million to Craftwood Lumber to settle a suit alleging a TCPA violation by sending over 1,500 advertisements via fax. And, Bank of America agreed to pay $32 million for violating TCPA through its use of auto-dialing technology and prerecorded voice messages without prior written consent.

TCPA has no cap on total damages—making it easy to imagine that an organization with a large roster of donors or potential donors could quickly expose itself to losses in the range of multiple millions of dollars.

How do you protect yourself from this exposure? Simple—get written consent from individuals before marketing to them via phone or fax.

State Data Breach Laws

Almost every U.S. state and territory has enacted laws requiring entities to protect sensitive consumer and employee information in their possession and, if that protection fails, to provide notification to the individuals so she or he is able to be alert to identity theft and fraud. These laws vary, but it is important to note that an entity must be informed of the evolving state laws that apply where their employees, customers and prospects reside

and not just where the entity is located. These requirements were initiated in 2003 with California's law with other states following suit. Some states have also already updated their original laws to keep up with current technology standards and consumer expectations. With identity theft continuing to rise and awareness increasing, the trend will certainly continue.

Increasingly, state laws address issues beyond breach notification. Some states require specific security measures such as a written information security plan or encryption. At last count, four states had specific requirements for a written information security plan, three states require a dedicated employee responsible for information security and seven states require security provisions in supplier contracts. Penalties for violations can range up to $500,000.

Some states require privacy policies to be posted. For example, since 2003 the California Online Privacy Protection Act (CalOPPA) has required that all websites that collect personal information about state residents post an online privacy policy if the information is collected for the purpose of providing goods or services for personal, family or household purposes. Most websites, even if not required, post privacy policies. Ensuring the privacy policy complies with applicable laws is a critical first step. It is important then to align technology and operations with the public-facing statements and to maintain that alignment as new systems and processes are adopted and the business grows. Some state laws even address internal privacy policies. In 2005, Michigan began requiring employers to publish internal privacy policies to address the proper handling of employee sensitive information. New York has adopted a similar statute as has Connecticut, Massachusetts, and Texas. As mentioned, states are working to keep pace with technology changes and evolving standards, which makes it important for entities to remain alert to developments.

An entity must be informed of the evolving state laws that apply where their employees, customers, and prospects reside.

General Data Protection Regulation (GDPR)

U.S. entities may, understandably, not be aware of developments in European privacy law. But, Europe recently made dramatic changes to its data privacy laws which will impact the way many U.S. entities do business. U.S. entities doing business with or within Europe (EU) or marketing goods and services (even if unpaid) to EU residents must update how they collect, handle and secure information that identifies a natural person, such as name, address or email address, or they risk facing heavy fines and penalties. Even entities that are not located in the EU may be impacted as their EU clients and suppliers may require compliance as a condition of continued business. This new regulation goes into effect on May 25, 2018, and contains important new operational requirements concerning data minimization, accuracy, accountability, purpose and storage limitations, and data protection that will require impacted organizations to begin making technology and administrative changes far in advance of the deadline.

The regulation also mandates that entities demonstrate compliance, which will require the creation of policies, procedures and documentation mechanisms. If your entity possesses data on EU residents, you are positioned to be impacted by this new regulation. If you market to or solicit donations from the EU market, you'll want to stay tuned to updates to the ePrivacy Directive (this is also called the "Cookie" Directive) which is expected to create as much disruption for U.S. entities.

The GDPR authorizes regulators to levy remarkably steep fines in amounts exceeding €20 million or 4 percent of annual global revenue, whichever is higher. Germany and Spain have stated openly that they may move against U.S. entities quickly. France has mentioned codifying parts of GDPR earlier than 2018. Some example requirements likely to be of interest to nonprofit entities include the following:

- Consent must be "freely given, specific, informed and unambiguous." Silence, pre-ticked boxes or inactivity is not sufficient to provide consent. Much of the data currently in use was collected using "opt out" mechanisms. This will need to be remediated if the information is going to continue to be retained and used.
- If the data is being used because consent has been given, then that consent must be able to be withdrawn at any time and withdrawn "as easily as it was given." This will necessitate changes in processes and quite possibly technology in order to accommodate. This also means that the data belonging to that individual

not only cannot be used going forward but must be erased.

- For data being used based on consent, the data subject has the right to request an inventory of all of the information an entity possesses on that individual. Accommodating these requests will require entities to establish mechanisms for receiving the requests, verifying the identity of the requestor, accurately and completely finding all relevant information to respond to requests and a documentation mechanism.
- A new "accountability principle" makes those that collect and use data responsible for demonstrating compliance with the general principles outlined in the regulation. (Demonstrating compliance is in the form of policies, procedures, impact assessments, documentation of consent, inquiry handling, responses and decisions, etc.)

Interpreting GDPR requirements strictly is likely to lead entities to incorrect conclusions. Special provisions for nonprofit organizations are present in the GDPR, but they are limited, so most of the regulation still applies to nonprofit entities just as it does for for-profit companies. Privacy rights are not absolute, and a balancing decision must be made by legal counsel familiar with EU privacy laws. The GDPR contains many different requirements and the requirements may or may not apply to all entities depending on various factors. To make correct decisions, counsel must know details on what data is processed, the circumstances around the original collection, what is done during processing, retention/disposition, access, security controls and onward transfers.

Data privacy is increasingly important and can, if ignored, have tremendous impact on a nonprofit. An annual privacy assessment is recommended to see that your technology, policies and operations are aligned with current applicable requirements.

For more information, contact Deena Coffman, managing director, BDO Consulting Technology Advisory Service, at dcoffman@bdo.com, or email CapinCrouse at info@capincrouse.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.