Nonprofits and Privacy Practices

Hugh J. Paterson III

University of Oregon

i@hp3.me

6 December 2021

Version: Class Submission

Within the context of the University of Oregon's PPPM 588 course, law is presented in an informative framework for potential managers to consider as they evaluate risk management. In this paper on *nonprofits and privacy issues* I take an overview perspective of privacy, specifically as it relates to data. This is a topic which was only briefly touched upon through the course content. I present an original paper looking at data privacy regulations and frameworks, along with some recommendations which nonprofit management should consider as they assess and mitigate risk imposed by their operations.

Abbreviations

CCPA	=	California Consumer Privacy Act
CCR	=	California Code of Regulations
CFR	=	Code of Federal Regulations
CPA	=	Colorado Privacy Act
DPO	=	Data Protection Officer
EU	=	European Union
FAQ	=	Frequently Asked Questions
FERPA	=	Family Educational Rights and Privacy Act

FOIA	=	Freedom of Information Act
GCHQ	=	Government Communications Headquarters
GDPR	=	General Data Protection Regulation
HIPAA	=	Health Insurance Portability and Accountability Act
IRS	=	Internal Revenue Service
NFL	=	National Football League
NSA	=	National Security Agency
UK	=	United Kingdom
USA	=	United States of America
VCDPA	=	Virginia Consumer Data Protection Act

1 Introduction[1]

Several US states have recently enacted consumer privacy laws.[2] These laws affect how organizations must interact with people and the contractors they use to process data. This also applies within the nonprofit sector. Further, internationally reaching laws like the European Union's *General Data Protection Regulation* (GDPR) have ramifications for nonprofit and for-profit companies within the US context (both based in the US and operating abroad). In this paper, I situate the application of these "data privacy" laws within the world of nonprofits. I discuss how nonprofit managment needs to account for these regulations in their risk assessment and administrative processes. Establishing good practice in response to existing laws will position nonprofits to continue to build trust with their constituencies as they carry out their corporate agendas. Privacy practices need to encompass not only statements regarding cookies on webpages, but need to look at how nonprofits process all data and contract with service providers for actions on data, including donor and mailing lists.

[1] My apologies, citing and referencing legal decisions is an art in which I am not well versed. Inevitably there are some formatting errors. I hope this is excusable.

[2] California 2018, Virgina 2021, Colorado 2021, California 2021 (a second law).

2 Background

Many governments acknowledge an operational space between where and how the government operates and where and how for-profit companies operate. Often governments designate different legal categorizations and requirements for companies operating in this inbetween space (Frumkin 2002). In the United States, the legal vehicle is the nonprofit corporation which is generally tax exempt via procedural arrangements governed by state requirements and the federal tax authority — The Internal Revenue Service (IRS).

Like all companies, nonprofits seek to mitigate risk and liability to their organization while still maintaining revenue streams and accomplishing their organizational priorities. One evolving area of risk management is the area of privacy. Broadly construed, privacy is a vague notion. In a personal context, privacy often relates to how two individuals treat each other, what they reveal about each other, and how they connect or convey what they know about each other to other third parties. The broad notion of privacy has made its way into legal codes which define specific liabilities and requirements on organizations. This creates a specific legal requirement on organizations, sometimes including nonprofit organizations. However, for nonprofit organizations there is a special consideration for privacy issues. Unlike for-profit businesses which traditionally function on the premise of offering a good or service over the cost price for the benefit of the corporation owners, nonprofits often are in the position of soliciting revenue for the purpose of delivering a service to a non-paying beneficiary while maintaining a cost-neutral balance sheet for corporation stewards. This variation in revenue generation often puts nonprofits in a position where they incur risk to their revenue streams due to the changing nature of public sentiment about their brand.

For some time privacy has been an issue in the public consciousness and one of political opportunity. This has had several compounding effects socially and practically on nonprofits. The first is that the general populace has found it fitting to advocate for more privacy rights, and second that politicians have used this sentiment to consolidate political advantages and pass new legislation regarding “privacy”. The confluence of public opinion and legal obligations adds a unique lens to the risk management assessment perspective. In contrast to the public service virtues which are often foundational and formative to nonprofits, modern business practices have

argued that nonprofits can be “more efficient” or “secure their sustainability” by securing their intellectual property and creating revenue streams around that property.[3] Nonprofits are often put into situations where they must evaluate their sustainability plans in the context of social “trust building”.

Within the United States the 4th amendment protects against unreasonable search and seizure.[4] Many have assumed that this constitutes a right to privacy. However, the amendment only effectively limits United States government functions — not commercial practices or the practices of other national entities operating in US territory. As the Snowden leaks revealed (2013–2014),[5] other countries' activities within the United States are not inhibited by the 4th amendment. More recently though are the practices of the government to rely on corporate information collection,[6] or information collected about people in the United States offered on the open market via individuals and companies (2015–2017).[7] Functionally in the United States, this workaround of the 4th amendment has added fuel to the public “debate” around privacy and the race to innovate solutions and legislation which limits data exposure via the *Third-Party-Doctrine*.[8] But many in the general public within the United States have become aware of privacy legislation through the international response to the European Union's GDPR (passed in 2016, enforced in 2018). The most noticeable and often the stereotypical interpretation of “data privacy” is what happens to the records pertaining to website visits. However, this is only a small portion of data privacy.

---

[3]Pressures to conform to modern business practices come from within the nonprofit management community, the community of nonprofit funders, and from the for-profit business community, cf. Mancha, et al. (2021) and Wang, et al. (2010).

[4]U.S. Const. amend. IV. https://www.law.cornell.edu/constitution/fourth_amendment

[5]The evidence suggests that, in some cases, British intelligence (GCHQ) was conducing signal gathering in the USA with US government agencies overlooking these activities, but also benefiting from and accessing data collected as part of these operations. Meanwhile, US operatives under the NSA were operating in the UK with the UK turning a blind eye to the operations but also benefiting from the shared data collected (The Libertarian Research & Education Trust n.d).

[6] The case of Zachary McCoy in Gainsville, FL (Schuppe 2020) demonstrates a general pattern in law enforcement to rely on the data provided to third parties. This pattern and the legal implications for privacy are well discussed (Lynch 2021; O'Brien 2021; Panduranga, Hecht-Felella and Koreh 2020).

[7]Between 2019–2021 several news outlets (among others, Thompson and Warzel 2019-12-19, Morrison 2020-12-2, Cox 2021-1-22) reported on FOIA request which resulted in evidence that government agencies were purchasing real-time or near-real-time data for cellphone locations. Vendors such as Ventel and others were often the the primary providers of such information. Buying access to information is different than asking for it from the source (in this case mobile carriers).

[8]*Third-Party-Doctrine*, is a legal doctrine within the US legal system which states that a person “has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” The foundational case for the third party doctrine is: *Smith v. Maryland, 442 U.S. 735, 743–44 (1979)* https://supreme.justia.com/cases/federal/us/442/735. In general instruments of negotiation (bank records, and other record types) have not been granted 4th amendment privacy considerations. There are some limits to the third party doctrine as established for geo-location information related to mobile phones in the case *Carpenter v. United States, No. 16-402, 585 U.S. ___ (2018)* https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

3 Applicability

Nonprofits in the United States have many different kinds of social impact missions and serve a large variety of beneficiaries. Large sports organizations such as the NFL are nonprofits along with small neighborhood focused food banks. Multi-billion dollar *Political Action Committees* which produce and distribute media for political campaigns along with libraries, museums, archives, churches, secondary and tertiary educational organizations, veterans support organizations, medical patient care organizations, open news reporting organizations, often fall within the range of organizations which are covered by the USA construct of nonprofit. These organizations all have different relationships with their constituencies (funders, beneficiaries, and partners). Many engagements with constituents produce a data trail which, to the right payee could represent a secondary profitable exchange of information between the nonprofit and the buyer of information.

Within the United States information in the form of data is construed as intellectual property and therefore often falls under property laws. These laws generally favor those who create the record of the interaction rather than all the parties involved in the interaction. This is starkly different from how the GDPR framework treats data about a person. That is, the EU treats personally identifying information as a personal possession of the individual regardless of who creates the data, and then the EU gives the individual the perpetual irrevocable right to regulate the data's use and distribution.

Just because the United States does not treat the data as the property of the individual, doesn't mean that there are no restrictions on the use of data. For instance, educational institutions risk losing their federally provided funds if they release certain student data,[9] and HIPAA [10] protects and defines the data sharing relationship between healthcare providers and insurance agencies. A common approach within the United States is to sectorize legislation and limit the scope of “protected” transactions around data. This creates an evolving system of regulation and patchworks of regulations which will continue to evolve (and lose efficacy) as the market evolves. Staying apprised of these evolving issues remains a challenge for all organizations. However,

[9] *Family Educational Rights and Privacy Act (*FERPA*) (20 U.S.C. § 1232g; 34* CFR *Part 99)*

[10] Health Coverage Availability and Affordability Act of 1996, 110 Stat. 1936 U.S. Statutes at Large & US Public Law 104-191 https://www.govinfo.gov/content/pkg/STATUTE-110/pdf/STATUTE-110-Pg1936.pdf For, information about the law see: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

nonprofits, startups, and other small organizations often feel the weight of regulatory chaos. Within the last two years three states have passed new privacy laws, one of which will impact nonprofits.

3.1 Strategic response

Nonprofits should seek to address these issues head on by appointing a data privacy officer (DPO). The role of a privacy officer goes beyond the creation of an organizational privacy policy[11] as has been recommended practice for nonprofits in the past. In the GDPR framework[12] the DPO reports to senior leadership, cultivates a corporate culture of data privacy, evaluates data handling procedures, security threats, data breaches, and brings expert knowledge of relevant law and regulations to the data handling practices and responses of the organization. The GDPR only requires this position for certain kinds of organizations. However, unlike most US laws the GDPR is extraterritorial. This means that violations outside of the EU could have consequences for subsidiaries of organizations inside the EU. Additionally, the rights bestowed on individuals by the GDPR apply to citizens and non-citizens physically located within the EU, and to persons who later become citizens in countries in the EU. For nonprofits which work internationally or have data about constituency members who are citizens of EU countries, violation of EU law could bring about severe financial consequences and also bad press.

3.2 New US laws

Within the United States a variety of laws have been enacted which address privacy issues. No federal law exists which covers all areas of data generation, data use, or data access (or licensed use via third-party-doctrine). Recent laws which have been enacted are often claimed to be "GDPR like", however, significant differences exist. For example, the GDPR vests rights of privacy in the person and grants these rights on the basis of the person's location within a EU member state and their citizenship; US state laws generally only apply to residents or businesses doing business in the affected jurisdictions. Three specific laws that have newly been passed include: the *California Consumer Privacy Act* (CCPA, passed 2018, enforced 2020), the *Virginia Consumer Data Protection*

[11] 11 CCR § 999.308 does address what should be in a privacy policy with regards to California law. However, broader best practices should be sought out. It is not entirely clear if 11 CCR § 999.308 applies to nonprofits as the *California Consumer Privacy Act of 2018* does not apply to nonprofits.

[12] GDPR Article 37: https://gdpr-info.eu/art-37-gdpr.

Act (VCDPA, passed 2021, enforced 2023), and the *Colorado Privacy Act* (CPA, passed 2021, enforced 2023). The exact definitions of the roles (data processor, data holder, consumer) and the kinds of data (personally identifying data, publicly accessible data, anonymized data, etc.) protected by the various laws, and the persons granted these rights vary across jurisdictions. Exemptions from adhering to the requirements of the law also vary. Nonprofits are currently exempted from the CCPA and the VCDPA, but are not exempt from the CPA or the GDPR.

3.3 Consumer rights

Broadly, the following rights are afforded to individuals, but reserved to state attorney generals to bring legal action under the laws: the right to confirm data that an organization may have including the categories of data, the right to correct any data, the right to delete data, the right to obtain the data, the right to opt out of any processing of the data, and in some cases a right from any discrimination on the bases of rights exercised. A fiduciary perspective of data stewardship as advocated by Balkin (2020) if adopted by nonprofit management would seek to honor these rights for clients, donors, beneficiaries, and customers regardless of which state they reside in or for the legal reason to offer these options to their constituency. Table 1 summarizes these rights across the three US laws presenting a high level overview. The table is complied from sources as indicated in footnote 13.[13]

[13]CCPA: California Civil Code, Division 3, Part 4, Title 1.81.5. §1798.100–1798.199.100
https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
VCDPA: From Code of Virginia Title 59.1, Chapter 52 § 59.1-573 through § 59.1-581
https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+SB1392ER
CPA: From Colorado Revised Statutes § 6-1-1306 & Final Fiscal Note:
https://leg.colorado.gov/sites/default/files/documents/2021A/bills/fn/2021a_sb190_f1.pdf

Table 1 *A comparison of rights across three new state laws.*

Rights	CCPA	VCDPA	CPA
To Confirm	The right to know about the personal information a business collects about them and how it is used and shared;	To confirm whether or not a controller is processing the consumer's personal data and to access such personal data;	Right of access to confirm that the controller is processing the consumer's personal data;
To Correct	Yes see §1798.106	To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;	Yes
To Delete	The right to delete personal information collected from them (with some exceptions);	To delete personal data provided by or obtained about the consumer;	Yes
To Obtain	In some cases	To obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means;	Right to data portability, which allows a consumer to access the data in a portable format.
To opt out of	The right to opt-out of the sale of their personal information;	To opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.	Right To Opt Out - Including the right to opt out of already opted in choices. (a) targeted advertising; (b) the sale of personal data; or (c) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.
Non-discrimination	The right to non-discrimination for exercising their CCPA rights.	——	——

3.4 Affected businesses

Not all businesses are affected by the requirements of state privacy laws. Unlike the GDPR which applies to all businesses due to the powers being vested as rights in the individual, the US laws have many exemptions and are framed in the context of transactional limitations on exchanges of data. Setting aside exemptions mentioned in the legislation, the following summaries indicate that many nonprofits may not be subject to them, if they don't have contact lists over 25,000 people.[14]

3.4.1 CCPA

The CCPA applies to for-profit businesses that do business in California and meet any of the following:

- Have a gross annual revenue of over $25 million;
- Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or
- Derive 50% or more of their annual revenue from selling California residents' personal information.

3.4.2 VCDPA

The bill applies to all persons that conduct business in the Commonwealth and either:

- Control or process personal data of at least 100,000 consumers or
- Derive over 50 percent of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers.

[14]Section 3.4.1, section 3.4.2, and section 3.4.3, are quoted from sources. The section on the CCPA from https://oag.ca.gov/privacy/ccpa, California Attorney General's FAQ question #5. The section on the VCDPA from the bill summary at: https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392. The section no the CPA from the fiscal note accompanying the bill at: https://leg.colorado.gov/sites/default/files/documents/2021A/bills/fn/2021a_sb190_f1.pdf.

3.4.3 CPA

The bill applies to a controller that conducts business in Colorado or produces products or services that are intentionally targeted to residents of Colorado and:

- Controls or processes the personal data of 100,000 or more consumers per year; or
- Derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more.

4 Conclusion

In this paper I have provided a comparison of consumer rights provided by three US state "privacy laws". Also shown are the variation in the applicability of the three laws. Not all of the privacy laws apply to all types of organizations. Nonprofits need to consider the application of laws in the states in which their constituencies reside, not only the state in which they are chartered. The 2017 decision of *South Dakota vs. Wayfair et al.*[15] removed the physical requirement for physical nexus. This means that the laws of the state of both parties in a transaction apply not just the laws of the physical location of the business/organization. The removal of physical nexus requirements has already impacted nonprofits by requiring them to register in states simply by adding a "give" or "donate" button to their website, cf. Liazos (2000) and Harbor Compliance and National Council of Nonprofits (2017). Nonprofit managers should anticipate that state laws will be interpreted to apply to cross-state transactions for the foreseeable future.

References

Balkin, Jack M. 2020. The Fiduciary Model of Privacy. *Harvard Law Review Forum* 134(1). 11–33.

Cox, Kate. 2021-1-22. Military intelligence buys location data instead of getting warrants, memo shows. https://arstechnica.com/tech-policy/2021/01/military-intelligence-buys-location-data-instead-of-getting-warrants-memo-shows (2021-12-08.)

Frumkin, Peter. 2002. The Idea of a Nonprofit and Voluntary Sector. *On being nonprofit: A conceptual and policy primer,* 1–28. Cambridge, Mass: Harvard University Press.

[15]Decision available at: https://www.supremecourt.gov/opinions/17pdf/17-494_j4el.pdf.

Harbor Compliance and National Council of Nonprofits. 2017. *Charitable Solicitation Compliance: An explanation of state charitable registration requirements.* Harbor Compliance & National Council of Nonprofits. https://www.harborcompliance.com/information/charitable-registration

Liazos, Melissa G. 2000. Can States Impose Registration Requirements on Online Charitable Solicitors. *University of Chicago Law Review* 67(4). 1379–1407. https://heinonline.org/HOL/Page?handle=hein.journals/uclr67&id=1385&div=gma&collection=

Lynch, Jennifer. 2021. Modern Day General Warrants and the Challenge of Protecting Third-Party Privacy Rights in Mass, Suspicionless Searches of Consumer Databases. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3908755

Mancha, Rubén, David Nersessian and John Marthinsen. 2021. Reorienting the sharing economy for social benefit: the nonprofit digital platform business model. *Social Responsibility Journal* ahead-of-print(ahead-of-print).

Morrison, Sara. 2020-12-2. CBP, DHS, and other government agencies are buying cellphone location data. Lawmakers want to know why. https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel (2021-12-08.)

O'Brien, Tim. 2021. New Writs of Assistance: Geofence Warrants and the Fourth Amendment. *SSRN Electronic Journal* . doi:10.2139/ssrn.3834623

Panduranga, Harsha, Laura Hecht-Felella and Raya Koreh. 2020. *Government Access to Mobile Phone Data for Contact Tracing.* New York: Brennan Center for Justice at New York University School of Law.

Schuppe, Jon. 2020. Google tracked his bike ride past a burglarized home. That made him a suspect. NBC News. https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 (2021-12-07.)

The Libertarian Research & Education Trust. n.d. The Snowden Revelations. Statewatch. https://www.statewatch.org/observatories/the-snowden-revelations (2021-12-07.)

Thompson, Stuart A. and Charlie Warzel. 2019-12-19. Twelve Million Phones, One Dataset, Zero Privacy. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html (2021-12-08.)

Wang, Zhongxian, Ruiliang Yan, Qiyang Chen and Ruben Xing. 2010. Data Mining in Nonprofit Organizations, Government Agencies, and Other Institutions. *International*

Journal of Information Systems in the Service Sector 2(3). 42–52.
doi:10.4018/jisss.2010070104