PRIVACY COMPLIANCE IN U.S. UNIVERSITIES

by

K Royal

APPROVED BY SUPERVISORY COMMITTEE:

_____

James Harrington, Chair

_____

Meghna Sabharwal

_____

Sarah Maxwell

_____

John McCaskill

To my heart and soul:

"In my daughters' eyes, I am a hero. I am strong and wise and know no fear.

Though the truth is plain to see, [they were] sent to rescue me.

I am who I'm meant to be in my daughters' eyes."

~ Martina McBride

Girls, without you, there would be no me.

And then there is one. The one who doesn't get anything I do, but he gets me. There were 14,000,605 ways this could've gone. And we found the one.

PRIVACY COMPLIANCE IN U.S. UNIVERSITIES

by

K ROYAL, BS, ASN, JD

DISSERTATION

Presented to the Faculty of

The University of Texas at Dallas

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY IN

PUBLIC AFFAIRS

THE UNIVERSITY OF TEXAS AT DALLAS

December 2021

ACKNOWLEDGMENTS

Thank you to my dissertation committee, led mostly by Dr. Doug Kiel through the years. In the end, we wound up with the perfect formula of expertise, guidance, understanding, and encouragement that every student should have. Thank you to the team that brought it home, my new chair Dr. James Harrington; Dr. Meghna Sabharwal; Dr. Sarah Maxwell; and Dr. John McCaskill. Also to Rita Medford, special thanks. We never met, but you are infallible.

Thank God. Literally. Nothing I do is possible without my Lord.

To my friends, who never faltered in their support, heard complaints and enthusiasm in mostly equal degrees, and always lent an ear, a shoulder, or a swift kick – unstinting and unrelenting to the very end. I hate to name names, but I will—Maggie, Wayne, and Nana just wouldn't stop nagging me. And Arthur, thank you for jumping in so quickly and excellently. But there is one in particular who truly stands out; Dr. Darra Hofman—the student who became the teacher. Thank you. *<Ummm, what's next, y'all? I'M D.O.N.E!>*

My family, unceasing, especially my mom. Without her, none of this would have been possible. Her confidence in me never wavered. To my daddy, you encouraged me to the very end. I wish you were here to call me Doctor, but princess was good enough for me. To Mum. You know.

November 2021

PRIVACY COMPLIANCE IN U.S. UNIVERSITIES

K Royal, PhD
The University of Texas at Dallas, 2021

Supervising Professor: James Harrington, PhD

Privacy law and compliance with those laws is a complex undertaking. This paper uses a mixed methods approach to review the scope and breadth of compliance with privacy laws at four-year universities in the United States. Starting with a Delphi method with privacy professionals defining the triggers for privacy laws, the laws most important for U.S. universities, and then the elements of a successful privacy program along with the risk factors for noncompliance, the researcher then examines publicly available information on a sample population of universities and lastly performs a legal review based on the Delphi findings and the Document Analysis. Both scholars and practitioners should find the paper useful. The outcomes identify what data subjects and activities trigger privacy laws at U.S. universities, what programmatic elements are required for a privacy compliance program to be successful, and what risk factors universities face in their privacy compliance efforts. All of this is reviewed through the Complexity Theory lens, considering both universities and privacy laws as complex adaptive systems.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

CONTEXT, SCOPE, AND INTENT

1.1 Introduction

The term big data is used frequently to refer to the astronomical growth of data that is generated, stored, and processed in the modern world, known by its volume, variety, velocity, and variability (Diebold 2019). The term encompasses the concept that the data sets are so big that conventional tools are inadequate to process the amount and complexity of the data being generated. It would take over 181 million years for an individual to download the current data from the internet (Petrov 2021). As a society, we have transitioned from an industrial economy to a knowledge economy (Castells 2000).

The amount of data, and particularly the vast unstructured data, has escalated privacy[1] concerns related to personal data[2] that is collected, manipulated, and retained (Wilson 2015). This is especially true given the number of personal information breaches that have occurred in conjunction with the amount of data being collected (RiskBased Security 2021). Yet the definition of personal data, the criticality of a data breach based on the sensitivity of personal data involved, and the harm to impacted individuals vary according to culture and law, with 128 out of 194 countries having privacy legislation in place (United Nations Conference and on

[1] The terms "privacy" and "data protection" are near-synonymous terms in mass media and among practitioners, although the concepts are not identical and are not used interchangeably in law. This paper will use the term "privacy" as opposed to "data protection" for simplicity, unless specified otherwise.

[2] At the time that privacy laws and jurisprudence became mainstream in the 1970s, and persisting today, there was no common understanding of what is meant by "personal information." In this study, unless specifically defined otherwise, "personal data" will be used instead of the term "personal information" or "personally identifiable information." Personal data comprises information that relates to or could be associated with an identified or identifiable natural person, whether the name of the person is included or not. This is also with the understanding that what could be used to identify a person fifty years ago was miniscule compared to the massive amounts of data that exist currently.

Trade and Development 2020). These laws vary in their application, strength, and scope. The strongest multinational privacy laws originate in the European Union (EU). In recent years, the EU passed the General Data Protection Regulation (GDPR) that entered into effect May 25, 2018. Prior to the GDPR, the EU was already considered the strongest multinational privacy regime (Krishnamurthy 2020). Now with its enhanced requirements, extraterritorial reach, and its penalties, the GDPR has become a major driver in global data protection.

Under the GDPR, sensitive personal data falls under "special categories" of data in article 9(1) being that which reveals ". . . racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (2018). Many other nations do protect sensitive personal information, but the determination of what is sensitive is relatively unique to each nation's culture. For example, in Israel, the Protection of Privacy Law of 1981 defines sensitive personal data as "data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person" (Protection of Privacy Law 5741-1981 1981).[3]

In contrast, the United States has no federal definition of sensitive personal data unless one considers that the sectoral laws themselves dictate what is sensitive. The importance of certain uses of personal data is clearly visible in the federal sectoral-based privacy laws that focus on healthcare, financial, and education activities and their associated personal data. In comparison to the first two sectors, the education sector has been largely ignored and this may be

[3] All laws referenced as a resource in this paper will have a full citation provided the first time it is referenced. Therefore, they will not be listed in the references section at the end of the paper.

due to myriad factors, such as the complexity of operations and structure at Universities and the amount and sensitivity of the personal data Universities process. Universities create, intake, use, share, and retain vast amounts of data, much of which are considered sensitive personal information. Insight into privacy laws applicable to these institutions and how they handle this data is not prolific, but there is a need for it to exist. "As higher education responds to increasing competition, technological changes, cyber threats, regulatory mandates, and pressures from stakeholders, the desires to seek innovative and effective risk management structures has never been greater" (Asante 2019, 14). This lack of available scholarship, coupled with complex influences and drivers, reinforces that this research is needed.

During the course of the research, the coronavirus pandemic (COVID-19) shut down many standard operating processes of the world and at the time of this paper, operating processes have still not returned to pre–pandemic levels and may never do so. Universities were no exception to the impact of COVID-19, and privacy became a concern as most people and entities shifted to a remote work environment, including remote education. In particular, institutions of higher education faced such issues as disease contact tracing, collection of new health data, concerns from constituents about the new uses of personal data, "Zoom bombing," and online proctored exams (Burns 2020). These issues did not herald the birth of privacy in the education sector, but they brought the issue of privacy to the forefront for individuals.

1.2 Statement of the Problem

"Cybercrimes and compliance-related incidents on campuses have rocketed in the past decade, mostly targeting sensitive organizational information and individual privacy. The trends and sophistication of attacks do not show signs of receding anytime soon" (Asante 2019, 14). This

dissertation addresses how institutions of higher education, specifically four-year universities in the United States (hereinafter "Universities"), are currently managing personal data given the ever-increasing number, scope, and breadth of privacy laws, regulations, or requirements (hereinafter generically referred to as "laws") that apply to personal data along with the exponential growth in the amount of data being generated and retained. This appears to be a relatively simple undertaking *prima facie*, but as this paper will demonstrate, it is very much a complex question, fraught with layers and nuances – signaling a topic ripe for investigation. This line of inquiry entails a multifaceted examination of the components (e.g., organizations, technology, and laws) within the context of the evolution from an industrial economy to a knowledge economy (Castells 2000) using an interdisciplinary approach, albeit with a focus on public administration and policy implementation.

This topic is further complicated by the lack of clarity about what privacy laws apply to Universities. For example, Universities which process personal data from the EU such as European students, activities with a European component (e.g., study abroad or EU-based satellite programs), and research participants or investigators, may be subject to the GDPR. Universities often provide some level of healthcare, which implicates the Health Insurance Portability and Accountability Act of 1996 (along with its subsequent amendments, HIPAA, Pub. L. 104–191, 110 Stat. 1936). These are only two examples of many privacy laws that may apply to Universities, as is explained in more detail below.

Lastly, the institutional settings themselves are challenging as Universities have unique characteristics as educational institutions on one level, but also diverge on an individual level. Managing any level of risk, including privacy, requires management at Universities to study and

understand their own practices and processes, stakeholders, internal and external influences, technology and systems, operational practices, size and complexity, and scope of influences (Asante 2019). Broskoske and Harvey identified seven challenges Universities face in implementing a new program; faculty issues, academic issues, marketing/competition, budget/fiscal, planning, personnel issues, and technological equipment (2000). Asante emphasizes that these challenges and "their impacts have multiplied over the years, making a case for higher education to put in place proactive management structures to deal with the challenges" (2019, 16). He emphasizes that Universities' risk exposure has amplified through their changes "in business processes, diversification of operations, efforts to comply with new regulations, designed transformations for competitive advantage, and increased global accessibility" (Asante 2019), 16).

1.3 Research Question

The overarching question that motivates this line of inquiry is:

How are Universities in the United States managing compliance with privacy and data protection laws? The answer necessitates three sub–questions:

1. What privacy laws apply to Universities?
2. What privacy program elements are critical to an effective privacy compliance program in Universities?
3. What are the common risk factors Universities face that impact their compliance with privacy laws?

Within the first sub–question, the applicability of privacy laws depends in large part on the criteria discussed above in describing the problem – identifying what personal data is collected and processed on what data subject and what activities the Universities are engaged in that would

trigger privacy laws. Under most privacy laws, one must consider the relationship of the individuals (data subjects) to the data and what is done with the data (the purpose or activity).

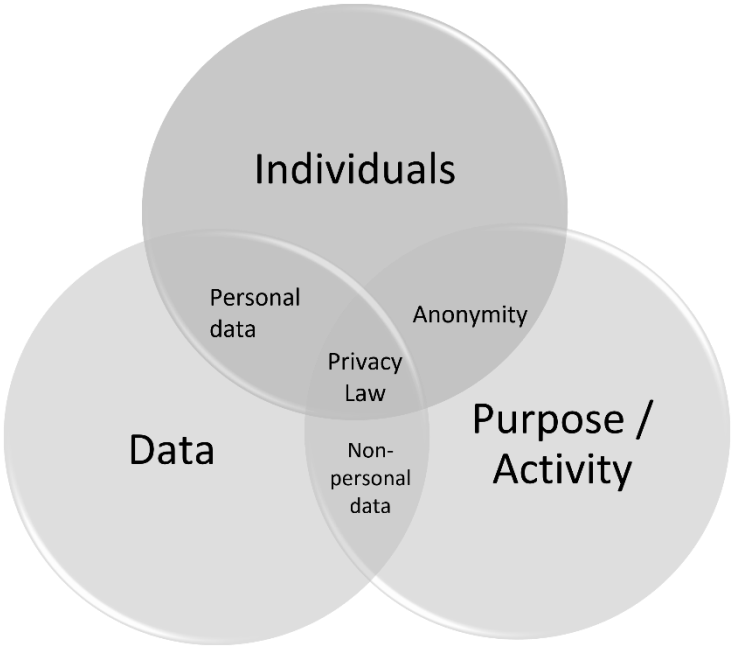


Figure 1: Privacy Venn Diagram

To understand privacy, one needs to first understand what qualifies as personal data. Figure 1 illustrates the intersection of individuals, data, and purpose or activity. Information on a natural person is personal data, regardless of whether the individual's name is included. In most definitions of personal data, any data related to or capable of being related to a natural person are considered personal data. This includes such elements as IP address, device ID, and online browsing history. Having individuals engaged in an activity but having no data on them equates to anonymity. Anonymity, as reflected in various data protection laws, such as the GDPR, is an incredibly high standard to meet especially in this era of big data. Anonymous data are incapable of identifying any individual and the data cannot be re–identified using any means (GDPR 2018, article 26). In many cases, the best outcome entities can reach is de–identified data or

pseudonymous data. De–identifying data removes personal identifiers, but the data are possible of being re–identified. Pseudonymizing data generally replaces identifiers with a code of some sort, a pseudonym, and must be protected under the GDPR (2018, article 25). The difference between de–identified and pseudonymous data is negligible for most uses. Lastly, using data for an activity or purpose without individuals included are non-personal data. This would not include pseudonymous or de–identified data, because individuals must be involved in those activities in order for the identifiers to be removed. In non-personal data, there are no identifiers because there were no individuals. Examples include "the United States won the most medals at the 2020 Olympics" or "the University of Texas at Dallas is located in Richardson, Texas."

The goal was to examine the compliance environment and needs of the institutions, the scope of legal requirements, and compliance implementation and oversight while ensuring the methodology followed a structured format to bring an objective perspective and academic rigor to the undertaking. The overarching goal was to marry the practical and academic side of the issue in order to provide a foundational understanding and formulate an approach that results in a consistent perspective that is replicable, leading to a maturity of the field.

1.4 Theoretical Framework

One theoretical framework encompasses these varying complexities, e.g. lack of clarity, multiple privacy laws, university structure, and compliance challenges: Complexity Theory. Complexity Theory in organizational studies is defined by the interactivity between and among actors and the feedback loops that influence actions and reactions. Complexity Theory seeks to explain a predictable set of activities that lead to unpredictable results. It allows us to understand diverse

systems through a cohesive lens, where traditional scientific methods fail (Grobman 2005; Zimmerman, Lindberg, and Plsek 2013). The results are unpredictable, which may lead one to consider the process chaotic, but Complexity Theory differs from Chaos Theory because the irregularity in the former follows certain rules that have been observed over time, which is the opposite of chaos (Zimmerman et al. 2013). A more thorough explanation of Complexity Theory is outside the scope of this writing. Instead, it focuses on how Complexity Theory has been applied to privacy law and Universities.

Universities have long been viewed as complex organizations as a whole, given their structure and scope of operations (Etzioni 1975; Mechanic 1962; Asante 2019), but as discussed below in the literature review, privacy law (or data protection law) is a complex adaptive system (CAS) itself (Zhang and Schmidt 2015). Given that this line of inquiry examines the management of legal requirements, it is a particularly apt observation as Pollitt states "that governments possess to an unusual degree is the power to alter the rules of the game—by legislation, the exertion of coercive force or by other means. It is as though the tiger can remodel the jungle" (Pollitt 2009). Likewise, organizations may also be complex adaptive systems if they are neither ordered or chaotic (Berreby 1996). Such examination is equally applicable to both public and commercial entities, plus universities have been well-established as complex adaptive systems (Martin 2019; Siemens, Dawson, and Eshleman 2018; Hadzieva et al. 2017). In essence, Complexity Theory is applicable on micro, meso, and macro levels.

Cohen explained, in 1999, that there are trends driving the adoption and interest in complex systems theories, including three trends that are directly applicable to this research. These changes include dramatic global changes impacting businesses and governments, such

as workforce diversity, local and global competition, continual innovation; the information revolution, where online engagement and data creation compress space and time; and the creation and dissolution of organizational entities on all levels, from the fall of nations to outsourced operations "as-a-service" (platform, software, infrastructure) (Cohen 1999). In addition, public affairs research leans towards qualitative research methodologies, this one being no exception (Rethemeyer and Helbig 2005; Grunig and Grunig 2001; Morçöl and Ivanova 2010).

Complexity theory is often used to contextualize complex system behavior, but there is movement towards using complexity as a methodological approach (Gear, Eppel, and Koziol-Mclain 2018). But Complexity Theory in itself is complex, often used alongside diverse frameworks to view recondite phenomena from a new or non-traditional perspective– the inherent goal of research (Eppel 2017). Turner and Baker explain that;

> Traditional sciences have utilized a reductionistic framework or a realist philosophy in which an entity is reduced to its smaller parts. By understanding the workings of the smaller parts, the whole can be understood more comprehensively. Although this reductionistic framework has served science well in the past, such as during the Industrial Revolution, it is inadequate to serve science well today due to the complexities of the modern world (e.g., increasing wicked problems, global warming, information overload, globalization, and geopolitical unrest). (Turner and Baker 2019), 2; internal cites omitted)

Building on the reductionist framework, complexity research expands the understanding of how the parts work within the whole system to understand how the parts work with each

other, potentially creating new systems and entities (Turner and Baker, 2019). Complex systems require a comprehensive approach. Attempting to understand complex systems on an individual level is inherently contradictory and defeats the goal of comprehending the whole of the system. Turner and Baker also tell us that "[n]ew theoretical models that reflect real-life complexity are being called for by researchers" (2019, 2; internal cites omitted). Although CAS theory is an element of complexity theory, it is robust enough to also stand alongside complexity theory as an independent yet entwined correlated theory.

The complexity theory appropriately contextualizes the organizational approach to privacy compliance for institutions of higher education. As Klijn states ". . . both rational behaviour and the assumption that the Government was a unified actor were more exceptions than the rule in the practice of public administration" (Klijn 2008), 300). Complexity theories stress that systems evolve in a non-linear and non-predictable manner, driven in large part by the independence of the actors within the system and the prevalence of multiple feedback mechanisms. Universities comprise a variety of actors (students, applicants, employees, professors, donors, etc.) and given how many Universities are embedded in their local communities, that there are also a variety of activities in which Universities engage (education, research, medical care, theater, sports, etc.). Universities are driven by their unique goals to their institutions, but also rooted in their respective histories causing inertia, most with deep ties to their communities and with constituents who are passionate about the university for personal reasons. Therefore, individual agent interactions and reactions are further complicated by not only rules and processes, but emotion. These are but a few

examples of the factors that are prevalent in Universities and in part why complexity theory applies.

Common Complexity Theory concepts include agents (individuals, collectives, or processes), nonlinear dynamics, feedback loops, coevolution, self-organization, emergence, boundaries, far-from-equilibrium, path dependency, and complex adaptive systems (Gear, Eppel, and Koziol-Mclain 2018). Although the full extent of complexity theory cannot be explained within this paper, this paper shall address aspects of complexity theory that are particularly relevant to Universities; self-organization, coevolution, nonlinear dynamics, and complex adaptive systems. Each of these will be discussed in more detail as applicable in this paper, particularly as the concepts aligned well with the Delphi method and the information gathered therein along with the subsequent findings driven by the Delphi. However, key to understanding complexity theory is understanding some of the basic elements.

The short sections below demonstrate where privacy law and compliance further complicate the circumstances. Viewing privacy law and compliance as a complex adaptive system in itself, operating within a complex organization drives the research approach of using complexity theory as the methodology behind structuring the research into the Delphi method, document review, and doctrinal legal research.

Self-organization

Self-organization is an apt description as it indicates the system is organized in a manner that it is wholly self-contained (Turner and Baker 2019). No other system or external influence controls the operations within the system, although localization within systems is not limited

by physical parameters, but rather the components of a system. Agents within the system interact with each other, forming relationships, building operational processes, and working together – creating organization within itself, by itself (Gear et al. 2018). This self-organization in turn drives the emergence concept listed above.

In the context of this study, Universities may be respective systems, and parts of the Universities, such as different campuses or departments are systems. Within these more obvious systems lie more subtle systems such as the privacy compliance systems. The privacy compliance systems may function as a layer across various internal systems, or they may overlap departments or locations. That is an element under consideration in this study. Privacy compliance may be self-organized as a privacy compliance program across the university as a whole or the privacy compliance system may be organized within self-organized programs, such as university medical centers who may have privacy officers who operate apart from the university.

Coevolution

Coevolution is the next step from self-organization. As systems interact and self-organize, they start to evolve (Gear et al. 2018). This evolution is unpredictable, cultivating diversity, escalating to new states of development, or producing new systems or patterns (Braithwaite et al. 2017; Allen, Maguire, and McKelvey 2011). As Universities, their divisions within, or their privacy compliance programs evolve, they are as likely to converge as they are to diverge – or even collide. We are watching Universities themselves evolve to comply with privacy law, but also their privacy programs - especially where the privacy programs are self-organized under the respective law driving the compliance need. With coevolution,

"…order emerges out of chaos and stability is punctuated by rapid change" (Cunningham 2004, 38). Privacy law is rapidly growing and therefore, compliance efforts to adhere to the requirements of privacy law are likewise growing.

Nonlinear dynamics

Dynamics in systems (or organizations) are not always stable. Dynamics can seem stable depending on the feedback mechanisms or temporary circumstances, but they can also destabilize quickly by varying factors (Klijn 2008; Mitleton-Kelly 2003). Within these dynamics, the instability itself may lead to success, providing the unstructured systems the ability to adapt. That ability, however, can further emphasize the aspects of self-organization and coevolution (Klijn 2008), the two other facets that seem to be most implicated in Universities.

Complex Adaptive Systems

Although CAS theory is often used to describe complex organizations, CAS is a critical element of complexity theory itself. Yet there is no singular definition of CAS, but rather an amalgamation that creates a concept that is recognizable by certain traits. One might be tempted to characterize CAS as chaotic, albeit there is structure and defined characteristics enough to differentiate CAS from chaos. A table of selected definitions is in Table 1, derived from Turner and Baker (2019), who also provided a compilation of CAS of over fifty characteristics derived from various scholars. In researching CAS to determine the definition that best applied to an understanding of privacy compliance, compliance programs, and how universities operate, the eight definitions presented below encapsulate the use and understanding of CAS throughout this study.

Table 1: Selected Definitions of Complex Adaptive Systems

Responsive processes among multiple agents. A complex adaptive system cannot be created or controlled by individual actors. But the system can be influenced, nurtured, and exploited by a group of actors.
A system of individual agents, who have the freedom to act in ways that are not always totally predictable and whose actions are interconnected such that one agent's actions change the context for other agents
Composed of interacting 'agents' following rules, exchanging influence with their local and global environments and altering the very environment they are responding to by virtue of their simple actions
A network of many agents acting in parallel, where control is highly dispersed, where coherent behavior in the system arises from competition and co-operation among agents themselves, where there are many levels of organization, with agents at one level serving as the building blocks for agents at a higher level, where there is constant revising and rearranging of their building blocks as they gain experience, where the implicit or explicit assumptions about the environment are constantly tested by the agent
Adaptive systems which consist of a variety of individuals with numerous relationships between each other, constantly interacting with one another, having mutual effects on one another, and thereby generating novel behavior.
A sub-set or type of system; has several properties that defy traditional science.
Different elements are continuously interacting with each other and producing reactions that are ultimately intertwined, but in practice are often impossible to anticipate or trace afterwards.
Social systems that are diverse, non-linear, consisting of multiple interactive, interdependent, and interconnected sub-elements. They are adaptive and self-organizing, tending toward ever-greater complexity operating at the 'edge of chaos' and therefore in a constant state of innovation and dynamic equilibrium.

In addition, CAS has defined characteristics, although scholars may not always agree on the precise list of characteristics. Turner and Baker provide a lengthy list of characteristics they gleaned from multiple sources (2019), These characteristics include adaptability, integration, fragmentation, concentration, schemas-diversity, emergence, non-linearity, strategic leadership, adaptive tension, enabling leadership, diversity, non-predictability, novel outcomes, boundary constraints, structure, complexity dynamics, feedback loops, and align choices for interaction (Turner and Baker 2019, 6–9). Although there are many more listed, as referenced above, this provides insight into why a system (or organization or systems within organizations, which will simply be "systems" hereafter) is complex, but useful and innovative.

1.5 Approach to Research

Developing the methodology used in this study to review and address the complexity of privacy compliance within a complex entity, two major factors drove the design: the need to use a structured, systematic research method and to respect the time constraints of the Delphi method expert participants as well as the sensitivity of any educational institution professionals addressing compliance requirements. This research required a mixed methods approach to

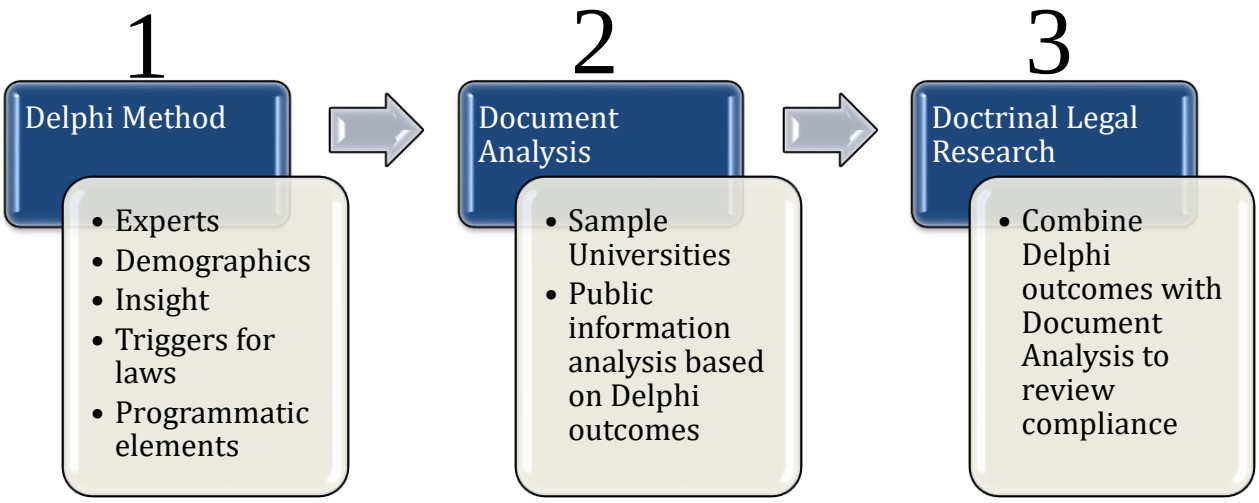


Figure 2: Research Plan

addressing the question, because the inquiry involves several avenues to reach the crux. Please see Figure 2 for a visual depiction of the overall research plan. The first consideration centered on removing bias. The researcher is an experienced global privacy professional, necessitating a level of academic rigor to be added to the methods to offset the bias of the researcher. Further information is provided in Chapter 3, but a panel of privacy professionals determined the elements of the detailed research rather than the researcher. The Delphi method adds that layer and directs the Document Analysis (Chapter 4) and Doctrinal Legal Research (Chapter 5).

There exists a reluctance by compliance and legal professionals to engage in studies that may expose non-compliance with applicable privacy and data protection laws.[4] However, as evidenced by the literature review and foundational overview section, the privacy compliance environment in university settings is quite complex and there currently exists no comprehensive structure or targeted systematic effort to assist these institutions in developing privacy strategies or achieving and maintaining effective privacy governance. Instead, government and private specialty groups have issued guidelines and frameworks that, while relevant, do not examine the complexities in managing such an effort nor do they lay out a specified set of activities to assist universities towards an optimal solution.

Next, the Document Analysis in Chapter 4 leverages the outcome of the Delphi method to drive the elements of analysis. This was combined with a sampling of Universities from both the public and the private sectors. A review of the available information determined the presence of the factors as identified through the Delphi method and then further combined to drive the Doctrinal Legal Research. The questions answered through Document Analysis are (a) whether the Universities are subject to privacy laws via identified triggers and (b) whether they have certain privacy program components and risk factors. The triggering factors reveal if the Universities are subject to certain privacy laws, whereas the programmatic elements and risk factors provide insight on their compliance activities.

The last chapter in this mixed methods approach is Chapter 5 on Doctrinal Legal Research. The findings of Chapters 3 and 4, respectively the Delphi method and the Document Analysis, coalesces into targeted research on privacy compliance activities at Universities in

[4] A research attempt before this one revealed privacy officers or counsel were leery of answering surveys about privacy compliance.

context of specific privacy laws. The goal of this research is not to determine if any particular university is legally compliant to their privacy obligations. Rather, the goal is to understand the landscape of privacy compliance in institutions of higher education, specifically U.S. public and private four-year universities.

1.6 Dissertation Structure

This first chapter provides the context, the problem being addressed, the research questions, and the research design in high level terms. Chapter 2 provides a targeted review of prior scholarship related to the facets of the research; first defining key terminology and concepts, then narrowing in on Complexity Theory and compliance. The next three chapters then focus on the three prongs of the research method as described above, respectively the Delphi method, Document Analysis, and Doctrinal Legal Research. Each chapter will present the research design, the findings, and a brief summary of that particular prong. Finally, Chapter 6 completes the research with a discussion of the findings and the limitations of the approach and studies. The chapter and this paper conclude with the significance of this research and the areas for future research.

CHAPTER 2

LITERATURE REVIEW AND FUNDAMENTALS

Privacy law has been examined extensively by legal scholars, starting with the well-recognized article “The Right to Privacy” by Samuel Warren and Louis Brandeis (Warren and Brandeis 1890). The full scope of privacy law is much too broad for this paper to cover; thus, it will focus on the subject of this research: privacy compliance in Universities. The privacy fundamentals provided herein in conjunction with the Doctrinal Legal Research in Chapter 5, will provide a review of current privacy law as applied to Universities. Given the scope of this line of research, there are three relevant strands of literature; privacy law, Complexity Theory as applied to privacy law and universities, and how institutions of higher education comply with law, particularly privacy law, including how they implement public policy. This chapter will address not only the foundational information on privacy that enables the reader to contextualize the research, but also the literature review.

2.1 Privacy Law Primer

Given the scope of this line of research, it is important to understand fundamental concepts about privacy law. This section presents a short overview on privacy, providing insight into the research so that the reader has a fundamental grounding in privacy prior to ingesting the work presented. Other than the Family Education Rights Privacy Act of 1974 (FERPA, 20 U.S.C. § 1232g; regulations at 34 C.F.R. Part 99) discussed further below, all other privacy laws applicable to organizations or activities in the U.S. apply to Universities as they do in the corporate sector. In addition, many for-profit and non-profit companies provide vendor services to Universities and depending on the legal reach of the laws, those laws that the Universities

must comply with also drive requirements for compliance in their vendors. Essentially, privacy professionals in the U.S. manage the same overarching range of privacy laws no matter whether they are employed by Universities, private companies, or the government. This section provides a history of privacy in the U.S., an overview of U.S. sectoral privacy law, and a brief view into state privacy law. Following the U.S. law, this section also presents a brief overview of applicable global law.

History of Privacy in the U.S.

Contrary to popular belief, the word "privacy" is not in the U.S. Constitution, although it is in eleven state constitutions. These eleven states are Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, New Hampshire, South Carolina, and Washington. Please see Appendix A for more details on the state constitutional law provisions.

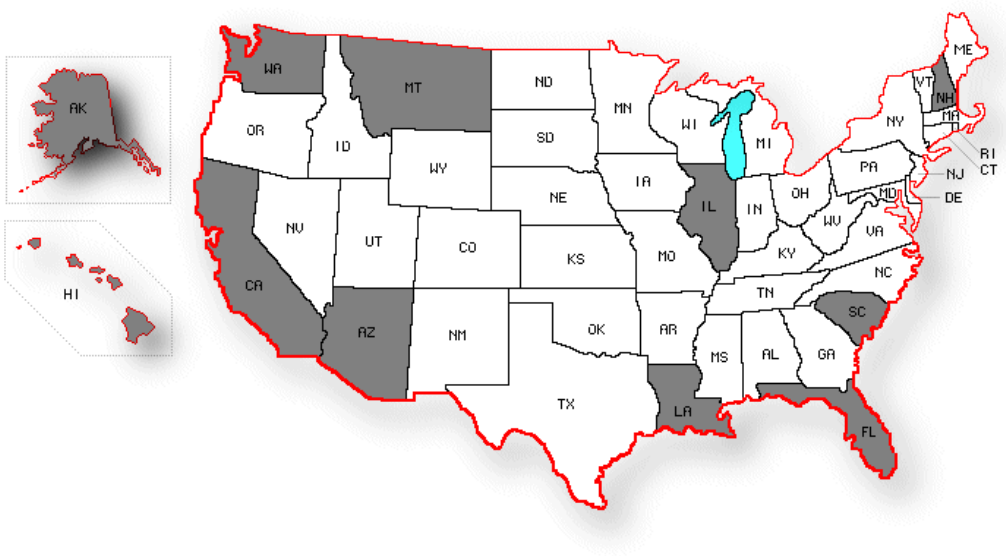


Figure 3: U.S. States with Constitutional Clauses on Privacy
(source: Free Maps online by DIYMaps.net)

Despite constitutional originalists who oppose inferring meaning to the original text of the Constitution, the recognition of a right to privacy has been well-established through a series of consistent rulings dating back through at least 1891 (see in chronological order of oldest to most recent: *Union Pacific Railway Co. v. Botsford* 1891; *Olmstead v. United States* 1928; *Skinner v. Oklahoma* 1942; *Griswold v. Connecticut* 1965; *United States v. Vuitch* 1971; *Eisenstadt v. Baird* 1972; *Roe v. Wade* 1973; *Doe v. Bolton* 1973; *Colautti v. Franklin* 1979; *Bowers v. Hardwick* 1986; *Ohio v. Akron Center for Reproductive Health* 1990; *Mazurek v. Armstrong* 1997; *Lawrence v. Texas* 2003; *Gonzales v. Carhart* 2007; *Carpenter v. United States* 2018). These are certainly not all of the rulings from the U.S. Supreme Court on privacy issues, but they merely provide a sample of significant cases. The key point is not that the U.S. Supreme Court always upheld the right requested, rather that the court always upheld that there is a constitutional right to privacy.

The critical turning point for cementing the constitutional right to privacy in the U.S. came with *Griswold v. Connecticut* (1965), wherein the majority declared in the oft-cited words of Justice William O. Douglas, that there are "penumbras" in the Bill of Rights which emanate from its specific "guarantees that help give them life and opinion. Various guarantees create zones of privacy" (*Griswold v. Connecticut* 1965, 484). Particularly, the U.S. Supreme Court has found that the spirit of various rights essentially incorporated privacy into the First, Third, Fourth, Fifth, and Ninth Amendments, as well as the Fourteenth. See Table 2. These include the right to privacy of one's beliefs in the First Amendment; privacy in one's home in the Third Amendment; privacy of one's person and possessions in the Fourth Amendment; and privacy of

Table 2: U.S. Constitutional Amendments Related to Privacy

Amendment	Text	Right
I	Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.	Privacy of Beliefs
III	No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.	Privacy of the Home
IV	The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.	Privacy of person and possessions
V	No person . . . shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.	Privacy of information
IX	The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.	Supports right to privacy by not excluding it
XIV	No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.	Right to liberty

one's own information or knowledge in the Fifth Amendment. The Ninth Amendment supports the right to privacy by not listing it as an exclusion. Lastly, the Fourteenth Amendment which contains the due process clause, and the equal protection clause is also interpreted to provide a right to privacy in the essence of the right to liberty. The decision also established privacy as a "fundamental right" (*Griswold v. Connecticut* 1965, 491), yet faced rebuke from Justice Hugo Black, an originalist, who opined "The Court talks about a constitutional 'right of privacy' as though there is some constitutional provision or provisions forbidding any law ever to be passed which might abridge the 'privacy' of individuals. But there is not" (*Griswold v. Connecticut* 1965, 508). Within less than ten years, the U.S. Supreme Court decided three major cases. In the

1967 case, *Katz v. United States*, the court faced a question of whether a search warrant was required to wiretap a public pay phone. Justice Potter Stewart infamously declared that the "Fourth Amendment protects people, not places" (389). Then in 1969, the Court unanimously concluded that the right of privacy protected an individual's right within his own home to possess and view pornography (*Stanley v. Georgia* 1969). In the *Stanley* decision, Justice Thurgood Marshall wrote:

> Whatever may be the justifications for other statutes regulating obscenity, we do not think they reach into the privacy of one's own home. If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds. (1969, 565)

Roe v. Wade followed in 1973, reinforcing the recognition of a right to privacy with the controversial issue of a woman's right to privacy of her body and decisions. Yet, as indicated in the *Stanley* opinion, the right to privacy emanating from the Constitution is not boundless. The privacy protections in the Constitution restrict actions such as searches and seizures by the government but are generally not applicable to private businesses.

The growing prevalence of privacy jurisprudence matched the growing body of statutory law. Looking at the global landscape, historians recognize the first data protection law in the world as enacted in the Land of Hesse in Germany in 1970, followed by the first national laws in Sweden in 1973, and in rapid succession: the United States in 1974, Germany in 1977, and France in 1978 (Burdon and Telford 2010; Bygrave 2008; Schwartz 2019; Solove 2006).

Specifically, in the U.S., the first privacy-related law was enacted in 1966, the Freedom of Information Act (5 U.S.C. § 552). This was quickly followed in 1970 with the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.) and the Bank Secrecy Act (31 U.S.C. 5311 et seq.) None of these were recognized at the time as "privacy laws" despite addressing critical elements of the Fair Information Practice Principles, which will be discussed in more detail in Chapter 5. However, 1974 saw the advent of two momentous privacy laws in the U.S., the Privacy Act (5 U.S.C. § 552a) addressing privacy in government interactions and FERPA.

Contemporaneously with the first development of privacy laws, and contributing to the concern around personal data, the world also experienced critical advancements in technology that had a profound impact on data collection, storage, and transmission. With the advent of the first desktop and mass market computers sold in the 1960s, (Computer Hope 2021) concern mounted around the world about protecting personal data.

U.S. Sectoral Privacy Laws

The U.S. laws that apply to personal data are sectoral based and generally require a person to be a consumer of certain services in order to qualify for protection of their personal data at the federal level. The four notable sectors in the U.S. with privacy laws include education, healthcare, finance, and public services. Each of these are discussed in more detail in Chapter 5 on the Doctrinal Legal Research. This section provides a basic grounding, to provide context – focused primarily on FERPA, followed by a brief discussion of additional U.S. privacy laws.

Although FERPA is the most significant and well-known federal law that applies to Universities, there are quite a few others aside from the other main sectoral laws, a brief introduction of each which is provided below. On the federal level, these include the Children's

Online Privacy Protection Act of 1998 (COPPA, 15 U.S.C. § 6501), the Federal Trade Commission Red Flags Rule (16 C.F.R. Part 681 2008), the Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510–2522 known as the Wiretap Act and 18 U.S.C. §§2701–2711 known as the Stored Communications Act), and the Federal Information Security Management Act (FISMA, 44 U.S.C. § 35 2002). This is, by far, not an exhaustive list. Some of these relate to information on students, but others relate to employees and to a lesser degree to consumers and vendors. To receive federal education funds, schools must agree to comply with FERPA (§ 99.1). This applies to all levels of education from early childhood through college and does not distinguish between private schools or public schools. In essence, FERPA restricts schools from disclosing education records without student authorization unless an exception applies.

FERPA defines educational records as those that are "directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution." (§ 99.3) FERPA includes several exceptions to education records including personal records used for recollection that are available to no one else, law enforcement records, personnel records related to employment by the school, certain medical records, and grades given by peers prior to becoming teacher-recorded grades. FERPA also defines personally identifiable information (PII) to include, but is not limited to, name (student and family members), address of student or family members, personal identifiers, and "other indirect identifiers" (§ 99.3). By itself, this is a broad definition of PII, because there are no qualifiers on who is a family member, and those other indirect identifiers include date of birth, place of birth, and mother's maiden name, but puts no finite limit on the category. In addition, FERPA includes both "[o]ther information that, alone or in combination, is linked or linkable to a specific student

that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty" and "[i]nformation requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates" (§ 99.3, definitions).

The federal sectoral laws in the U.S., aside from FERPA include those related to healthcare, financial data, and data processed by the federal government. These laws do overlap such as with government-owned health care facilities or financing offered by the hospitals for medical treatment or even the acceptance of credit cards for payment. Although HIPAA is not the only federal law that applies to health information, it is the most well-known, albeit misunderstood, federal law that addresses health care information.[5] It is also more comprehensive in the medical data it does protect than other federal laws which may also address medical information. HIPAA's privacy, security, and breach notification rules specifically apply to covered entities (health care providers, health plans, and health information clearinghouses)

[5] To understand how confusing HIPAA is for both professionals and the average person, please review information on HIPAA and vaccination records for COVID-19. For example, I wrote an article on "My Employer Can't Ask for Proof of Vaccination' and Other Myths Regarding COVID-19 and HIPAA" on September 7, 2021, for Corporate Compliance Insights. Available online at https://www.corporatecomplianceinsights.com/employer-covid-19-hipaa-myths/. Another example includes Representative Marjorie Taylor Greene (R-GA) who refused to answer questions on her vaccination status because it was a "violation of my HIPAA rights" for the reporter to ask according to Aaron Keller in Law and Crime, available online at https://lawandcrime.com/legal-analysis/lawmaker-marjorie-taylor-greene-in-ten-words-or-less-gets-hipaa-all-wrong/. The last example is the University of Texas at Dallas' online information on COVID at https://www.utdallas.edu/covid/response/faq/. There is a question on whether professors can ask students if they have been vaccinated. The response is "No, due to HIPAA Privacy Rule." According to the HIPAA Privacy Manual for the Callier Center posted at https://calliercenter.utdallas.edu/hipaa-privacy-manual/, UT Dallas is a hybrid entity, and more specifically, the Callier Center for Communication Disorders is a covered entity under HIPAA. Unless the professors are considered members of the workforce within the Callier Center, there are no HIPAA implications between professors and students. There are other reasons professors should not ask, and perhaps HIPAA is one way to scare them into not asking, but it is incorrect. It would be the same as a professor asking a student about missing a test due to illness. If there is no HIPAA in the latter, there is no HIPAA in the vaccine inquiry. There are many more examples in our daily lives about this confusion on whether HIPAA applies to all health information. This is simply a current topic.

and their business associates. The common misconception about HIPAA is that it applies to all health information, but it does not. HIPAA only applies to those covered entities who process certain information for certain electronic transactions, most of which involve benefits and claims (45 C.F.R. § 160.103, definitions).

Three other federal laws apply to health information – the Genetic Information Nondiscrimination Act of 2008 (GINA, Pub. L. 110–233), the Americans with Disabilities Act of 1990 (ADA, 42 U.S.C. §§ 12101–12213) both of which are health and employment-related, and the Federal Policy for the Protection of Human Subjects, known as "the Common Rule" (a 1981 rule of ethics revised in 2018 regulating research involving human subjects, encapsulated in the 1991 revision to the U.S. Department of Health and Human Services, 45 C.F.R. 46, Subparts A, B, C and D on Public Welfare). GINA prohibits genetic discrimination in health and life insurance and employment, where the definition of genetic information includes health information on family members. The ADA, especially as amended in 2008 (Pub. L. 110–325), defines disabilities and protects people with disabilities from employment discrimination. The Common Rule applies to federally funded research on human research subjects, and private research institutions may voluntarily agree to comply with the standards. The Common Rule sets out explicit standards for informed consent, a fundamental privacy concept and works hand-in-hand with HIPAA on the confidentiality of health information.

Moving to the financial sector, there are quite a few privacy laws. However, the main one is the Financial Services Modernization Act of 1999, (Pub. L.106–102, 113 Stat. 1338) more commonly known as the Gramm-Leach-Bliley Act (GLBA). The GLBA requires financial institutions to protect confidentiality and security of customers' nonpublic personal data (NPI),

such as Social Security numbers, credit and income histories, credit and bank card account numbers, phone numbers, addresses, names, and any other personal data that is not publicly available. Financial institutions under the GLBA definition comprise organizations who might not self-identify as a "financial institution" due to the broad scope of the definition. Any institution, no matter the size, that is "significantly engaged" in providing financial products or services, including nonbank lenders, qualifies as a financial institution (GLBA, § 313.3, definitions). In the case of Universities, certain activities might bring them under the scope of the GLBA, such as student loans and accepting donations.

Lastly in this federal sectoral portion, there is the Privacy Act of 1974 (5 U.S.C. § 552a), mentioned above, which applies to the privacy of personal data collected by federal agencies in the U.S., by establishing a "Code of Fair Information Practices." The Privacy Act addresses disclosure of personal data, requirements to access and amend personal data, and recordkeeping requirements. Yet, the Privacy Act does not apply to all personal data processed by the U.S. federal government. It only applies to federal agencies (the Privacy Act, 5 USC § 551(1)), such as the Federal Trade Commission (FTC) or the Department of Health and Human Services (HHS). This means that personal data processed by offices in the legislative or judicial branch are not protected by the Privacy Act. Most importantly, although the Privacy Act would not generally apply to Universities themselves, it does apply to the Department of Education, which is a federal agency. For example, the Department of Education maintains records of "[i]ndividuals who have made inquiries or who have filed complaints alleging violations of provisions in FERPA and [the Protection of Pupil Rights Amendment]; and those who have commented to the Department on its proposed rules and practices" (U.S. Department of

Education 1999). Thus, any students, employees, parents, or interested parties at Universities who file a FERPA complaint would have their information on file with the Department of Education, who would then communicate with the institution and complainant about the complaint, acquire records pertinent to the investigation, and maintain those records until they could be deleted.

State Privacy Law

During the course of this research, the first U.S. state passed an omnibus privacy act, the California Consumer Privacy Act (CCPA 2018) and then also passed the next version through a ballot initiative in 2020. The Consumer Privacy Rights Act of 2020 amends the CCPA but does not take effect until 2023. Multiple states had privacy laws proposed both in 2020 and 2021, but at this time, only two additional states have passed omnibus privacy laws, Virginia (Virginia Data Protection Act 2021) and Colorado (Colorado Privacy Act 2021) – both of which are structured based on the EU's GDPR.

Several states have their own privacy laws related to healthcare and one's physical identifiers, directly or indirectly. These include California's Confidentiality of Medical Information Act and the Insurance Information and Privacy Protection Act. Indirectly, the Illinois Biometric Information Protection Act along with similar biometric laws in Texas and Washington apply to biometrics, which are physical identifiers and considered by some to be a subset of health data. Although HIPAA would preempt any state laws that contradict its protections, states are permitted to pass laws with greater or complementary protections via the U.S. Constitution. The Tenth Amendment provides that "[t]he powers not delegated to the

United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."

Most states have regulations specifically relating to health professional or facility licensure that apply to medical records in such aspects as retention, security, and availability to patients. These may vary widely across states and are not consistently found in comparable areas of law. For example, some states may hold that physicians own the medical records while others dictate that hospitals do. Where medical records may be at a school clinic, it may then be unclear who owns the records. States also tend to regulate the privacy of records related to sensitive areas of health, e.g., sexually transmitted diseases or drug addiction treatment. In most cases, these targeted areas of law do not provide exceptions for institutions of higher education or more generally, non-profit or government entities which include most of the Universities targeted in this research effort.

International Privacy Law

There are well over 900 laws related to privacy around the world (Greenley-Giudici 2020). The EU leads in the regulation of privacy law, or rather, data protection law, and has done so for decades. The GDPR has influenced laws globally, as evidenced by Brazil's Lei Geral de Proteção de Dados Pessoais (LGPD 2020), and the aforementioned state laws. The critical aspect is that international privacy laws may apply to Universities. The impact of this research will be covered in the Delphi method and findings and also in Chapter 5 in the Doctrinal Legal Research.

2.2 Literature Review: Complexity Theory

As discussed *supra*, Complexity Theory provides a framework in which to consider the complex law and organizations at issue in this study. In this literature review, both privacy law and institutions of higher education were considered in terms of Complexity Theory.

Complexity Theory and Privacy Law

Complexity Theory has long been applied to law in general (see for example Hornstein 2004; Kades 1996) and specifically complex adaptive systems (CAS) has been examined as applicable to specific areas of law, such as the future of law (G. T. Jones 2007), judicial decision-making (Holz 2006), and U.S. healthcare law (Bloche 2008). However, in 2015, Zhang and Schmidt proposed that the subject matter of privacy law qualifies as a complex adaptive system. Their scholarship followed the 2013 revelations of Edward Snowden, a former Central Intelligence Agency employee and former contractor with the National Security Agency, disclosing the far-reaching surveillance activities of the U.S. government. Snowden's disclosure has impacted privacy law worldwide since that time (Butler and Hidvegi 2015). Suddenly, privacy was not merely a legal construct that nations interpreted differently, but one with significant import for national security that juxtaposed the interests of individuals against the interests of nations.

Zhang and Schmidt consider privacy law as a vast system in which large networks (individuals, companies, regions, nations) exist with diverse components, interconnected networks, with no central control over the entire body of global privacy law, that creates complex collective behavior, and is capable of adapting. They propose that the subject matter in review is not personal data, but rather "people's individual and collective behaviors related to

personal data" (2015), 202). Having actively worked on the Chinese data protection[6] environment as juxtaposed against the European model, the authors struggled to articulate a model that encompassed a variety of theories, including change theory, realism, positivism, innovation, and Chaos theory. Their conclusion landed in Complexity Theory, finding that using the CAS structure better describes and clarifies "the gaps between the dynamics of laws and of its subject matter than traditional legal theory (2015, 206).

Recently, Complexity Theory related to privacy arose in the context of adoption of a blockchain-based loan system (Sun et al. 2021). Although the authors did not arrive at this theory through the lens of privacy, but rather technology and innovation, their research focused on privacy concerns. This is evident in the risks they specifically identified, such as "Will so much information uploaded to financial institutions be used for tax investigation or employment arbitration?" or "Will senior employees who manage this information sell this information privately to peers for compensation?" (2021, section 5).

Thus, scholars are starting to recognize the complexity in privacy law, albeit some indirectly. At this time, the literature is limited in scope and application, but it is an emerging body of research that this paper seeks to help fill the void. If nothing else, it should contribute to the growth and perhaps the validity of the field.

Complexity Theory and Universities

There is ample literature applying Complexity Theory to educational institutions (Askew et al. 1997; Cunningham 2004; Louis and Miles 1991) and with such prevalent research, there have been equal amounts of contribution to the application or use of Complexity Theory in studying

[6] At the time this paper was written, the People's Republic of China issued its Personal Information Privacy Law (PIPL) in September 2021 with an effective date of November 1, 2021.

aspects of education or behavior at educational institutions. However, the literature is scarcer when narrowed to post-secondary educational institutions, albeit well-established. In large part, Complexity Theory has been applied to certain aspects of the education environment. For example, Complexity Theory has been used to understand and identify improvements in educational leadership (Hazy and Erogul 2021; Lichtenstein and Plowman 2009; Martin 2019; Morrison 2002), pedagogical approaches (Besley and Peters 2013; Cropley 2001; McGregor 2020), student outcomes (Hadzieva et al. 2017), and change management, especially technology adoption (Martin 2019; Russell 2009).

Of particular interest for this line of inquiry, Complexity Theory has also been applied to the operations of institutions of higher education, assessing whether universities are complex

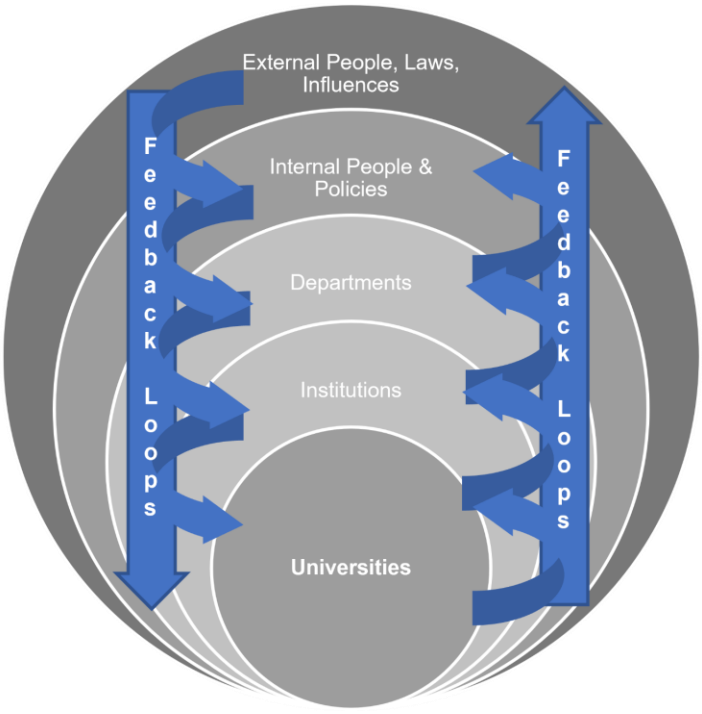


Figure 4: Multi-actor Influences in a University Setting

adaptive systems (Hadzieva et al. 2017; Jacobson, Levin, and Kapur 2019). As discussed by Martin (2019) Universities have multiple elements at play, from external influences such as donors and law to internal actors (employees, students, intercollegiate sports), from departments to various institutional settings (multiple campuses, satellite offices). Figure 4 provides a visual for these factors, including the feedback loops that may flow from one to another or throughout all levels.

Martin examined how to improve mathematics pathways because educational institutions were under pressure to improve student outcomes yet were struggling to move from piloting programs "to implementing reforms at a scale that supports every student's success" (2019, 57). This struggle can be extrapolated to nearly any program that needs to advance to system-wide implementation. Complexity Theory offers a conceptual framework, powerful enough to encompass and drive the "dynamics of transformational change in higher education systems" (Martin 2019, 58).

Universities are organizational systems comprising diverse and active individuals and departments ("agents") who interact and adapt due to the knowledge and experience they gain, plus the influences of the external environment, their values individually and as a community, and the formal rules adopted by the internal systems or the overall system (Keshavarz et al. 2010; Martin 2019). Martin also recognized that

. . . institutions of higher education are nested in a larger ecosystem of complex systems that dynamically exchange information and exert environmental pressures on one another. It is through the iterative feedback loops between the internal and external systems that the policies, practices, and cultural norms embodied by the institution emerge. (2019, 60)

An example of this is the University of California, which comprises ten campuses, five medical centers, three national labs, and thirteen research centers of which three are systemwide centers and six are multicampus centers (University of California 2020).

The four main factors that have been identified as critical for change to succeed in Universities are active initiation and participation, pressure and support, changes in behavior and belief, and the overriding problem of ownership (Fullan 2001; Louis and Miles 1991). Louis and Miles would add that effective coping strategies are the most important factor for change (1991). Whereas this paper stops short of identifying exactly how Universities might implement change, it is helpful to understand that change itself is also complex. Recognizing this up front will help Universities identify how to better manage privacy compliance should that the current management be deemed insufficient for the demands.

2.3 Compliance with Privacy Laws at Universities

Scholars have not examined privacy through one lens, they have used multiple perspectives to try to understand not only the concept of privacy but how that concept impacts individuals and organizations. There has been very little attention paid to privacy at universities in general, much less privacy at universities within the United States. In many cases there is scholarship on specific compliance topics at universities, but rarely on how to manage privacy as an organizational program within a university. Within the U.S., this may be because there is a defined area of law that specifically addresses education: FERPA. However, as also explained by the Delphi method, that is a short-sighted view. FERPA does not address all the privacy issues within a university setting.

It was not unexpected to find minimal literature on privacy compliance at Universities specifically. The primary distinguishing characteristic of privacy at education institutions is its applicability to the student population, some of which may not be adults, some are adults functioning as such away from home for the first time, and some may be within a vulnerable population. The issues, in general, are the same as with other public or private entities – that there are multiple privacy laws that may apply. This generalization about most federal privacy regulations also carries through to state laws and standards addressing privacy and security, such as the Payment Card Industry—Data Security Standards (PCI DSS). The latter is a set of standards required by the credit card companies that apply to all entities who accept credit card payments.

There is an increasing number of articles and examinations on certain aspects of privacy at universities, such as social media (Peruta and Shields 2017; Wang et al. 2020), distance education (El-Khatib et al. 2003; Jerman-Blažič and Klobučar 2005; M. L. Jones and Regner 2016), COVID-19 contact tracing or reporting apps (Mailthody et al. 2021), attorney-client privilege and legal issues (Sisk and Halbur 2010; Woods and Veil 2020), or violence on campus (Dowding 2011) – mostly in the context of FERPA. Departing from the U.S. aspect, there is more literature available. Avuglah and colleagues assess the privacy practices of academic libraries in Ghana (Avuglah et al. 2021) and Eroglu and Cakmak do the same for Turkish academic libraries (Eroğlu and Çakmak 2020) – both of which provide fascinating insight into the perils of the lack of privacy in libraries and digital content. In Canada, Dowding reviewed the Freedom of Information and Privacy Protection Act's impact on universities in Ontario (2011). Bentinck and colleagues looked at the perception of privacy in a Dutch university (Bentinck, van

Oel, and van Dorst 2020). Despite the increasing amount of literature, managing internal privacy compliance overall is not a topic that has been addressed specifically. One article that stands out by Christine Borgman in "Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier" (2018). She delves into some of the complexity of managing privacy at a university, however she does limit her examination to two specific topics: research data and what she terms "grey data."

Borgman, well known for her expertise in privacy in the field, does an admirable job of laying out the university responsibilities for data. She addresses stewardship and governance, the two topics that she focused on as well as the topics of privacy, academic freedom, and intellectual property. Further she looks at the Privacy Frontier. In this section of her article, she examines access to data, uses and misuses of data, public records request, cyber risk and data breaches, and cured rating data for privacy protection. The conclusions and recommendations address how in some instances, good stewardship means releasing data to the public and in other circumstances means keeping data from the public. She explains privacy by design (PbD), the code of fair information practice, the Belmont report, and codifications of academic and intellectual Freedom are established and tested. She does address that implementation is often incomplete. Borgman advises that "[l]ocking down all data less they be released under Open Access regulations, public records request, or breaches will block innovation and the ability to make good use of research data or gray data" (2018, 412). She emphasizes the need to embed the ethic throughout the universities, promoting joint governance, promoting awareness and transparency and lastly cautioning people not to panic. "The opportunities in exploiting data are

only now becoming understood. Balanced approaches to innovation, privacy, academic and intellectual freedom, and intellectual property are in short supply" (Borgman 2018, 412).

Once we turn to the issue of whether privacy laws outside the U.S. an impact on Universities, the literature narrows to the GDPR. Fearn and Koya look at the GDPR impact on universities in the United Kingdom (2021). Specifically, they look at learning analytics and big data on students post–GDPR. Their research starts with the premise that "it is irresponsible to believe more educational data always means better educational data" (2021, 165), and concludes that the GDPR has had very little impact on the collection and use of data, only the storage. Again, the research is limited to one aspect of data at universities.

Schwartz and Peifer (2017) take a clear legal approach to the analysis albeit across the data protection in general and not specifically the GDPR. They review the two regimes and history of the data protection development in both the U.S. and Europe, recognizing that the EU takes a protectionist stance while the U.S. "is interested in the free flow of data and access to the bounty from the consumer marketplace" (2017, 178). At this time, the U.S. and EU are at a small impasse for the free flow of data, given that the Court of Justice of the European Union declared the EU-U.S. Privacy Shield invalid as a data transfer mechanism in its July 2020 decision in *Data Protection Commission v. Facebook Ireland Limited, Maximillian Schrems*, commonly known as "Schrems II." This decision was primarily based on the extent of U.S. government surveillance activities, which do not guarantee a level of data protection for individuals equal to that of the EU under GDPR.

2.4 Public Policy Implementation

Another consideration is that privacy compliance includes implementing public policy. Review of public policy implementation has several aspects to consider. In general, research faces three classifications: the generation of study methodology, the single-case study vs. comparative approach, and regionalization (Saetren 2014). The first classification is the generation of methodology, distinct in its three divisions of 1960–1970s, 1980–1990s, and post–2000. The first generation is characterized as single-case study, qualitative, and a–theoretical, the second as empirical, theoretical, and comparative; and the current generation as a more advanced composition of the first two with a focus on methodology (Barrett 2004; Saetren 2014). As scholars have grown in their structure and rigor, accompanying research has benefitted in its contribution to the study of public policy implementation by considering both qualitative and quantitative data and an increasingly sophisticated theory-based assessment.

The second classification of single-case study vs. a comparative case study has not been a linear advancement, sacrificing longitudinal research in its search for comparisons (Saetren 2014). Single case studies have been sacrificed for comparable studies and with that, lost an aspect of the qualitative insight gained through evaluation of a single implementation but gained insight into more theoretical approaches. Several studies seek to combine the two by limiting the comparison numbers (Chunnu-Brayda 2012).

The third classification is based on region. By far, most studies into public policy implementation have been conducted in the U.S. with a steadily increasing number out of Europe, outpacing the U.S. production (Saetren 2014). Studies out of Europe, however, are less theoretical and more quantitative, and more comparative across nations (Bondarouk and

Mastenbroek 2018; Castellacci, Fevolden, and Lundmark 2014). Conceptually, this approach is geographically similar to multi-state comparative studies in the U.S. (Saetren 2014).

There are four factors interfering with the successful implementation of public policies. Barret explains that these four factors are lack of clear policy objectives, communication and coordination, value and interest differences between actors and agencies, and agency autonomy (Barrett 2004), 252). A lack of clear policy objectives permits differential interpretation and discretion in action. A multiplicity of actors and agencies involved in implementation creates a barrage of confusion and competing priorities. Problems of communication and coordination between the 'links in the chain' further reinforces that issue because of the relationships within and among organizations. The differences between actors and agencies are rooted in value and interest differences, a further dissolution of priorities. Without having the same priorities, perspectives compete and impact policy interpretations and motivations for implementation. Lastly, the relative autonomy among implementing agencies means each one has siloed administrative rights and enforcement (Barrett 2004).

Foreign policy issues, such as anti–bribery (Tarullo 2004) or more generally, external governance (Wunderlich 2012), reveals literature specifically about implementing foreign policy and compliance with such requirements. This extraterritoriality provision comes into play if laws outside the U.S. apply to Universities. In large part, however, many of the reviews are of a legal nature, citing foreign law and enforcement actions – very little is dedicated to public affairs. Although the interest of this research into privacy compliance of Universities is closely entwined with law, one element captured within the study was how certain foreign privacy laws have

extraterritorial applicability to institutions of higher education, such as the privacy laws of Canada, the EU, the United Kingdom, or Brazil.

The last line of policy implementation is specifically on laws that drive global change. Scholars have looked at influences on global public policy, typically both Europe and the United States. Europe's influence on the global market has been reviewed extensively (Bach and Newman 2007; da Conceição-Heldt 2014; Jacoby and Meunier 2010). In particular, the European influence has been reviewed as it relates to data privacy and financial market regulation (Bach & Newman 2007), although this review did not look at specific compliance by entities to foreign regulation, but more of a general review on the ability to drive global policy. Although outdated (Europe has moved beyond Directive 95 to implement the GDPR), it provides an overview of policy considerations for global implementation.

U.S. businesses desire to appear transparent about their data practices and (B. Gupta and Chennamaneni 2018). In part, if entities are subject to foreign jurisdictions that have privacy laws, such as the EU, then entities are required to implement those controls. Of course, "subject to" and "compliant with" are not synonymous. Plus, compliance deviations for local law are desired when the exception provides for a significant market advantage. This is especially true in a world where personal data is so readily available, simple to collect, and subject to massive manipulations that provide valuable insights. However, due to increased enforcement by the U.S. Federal Trade Commission (FTC) on deceptive trade practices and enhanced scrutiny from other jurisdictions, privacy is emerging as a market differentiator (B. Gupta and Chennamaneni 2018; Nehf 2007).

Further, businesses want to acquire and retain customers – and trust is a large part of the strategy (Langenderfer and Miyazaki 2009; Shey 2014). Analysts predicted that half of all business decision-makers in North America and Europe will view privacy as a competitive differentiator by 2018 (Shey 2014). This was not proven to be true in a general sense, despite claims to the contrary (Shey and Iannopollo 2018). However, privacy as a differentiator in the next [X] years is becoming a tireless prediction (Esposito 2021; Visconti 2018). Some companies have looked towards privacy and security to differentiate themselves from competitors in a tough market, while others are trying to recover from a privacy incident or capitalizing on a competitor's actions (Fazzini 2019; Shey and Iannopollo 2018). No claims of enhanced privacy have been identified related to Universities in the context of marketing or commerce, with the exception of special programs offered.

An additional driver for entities to implement privacy practices was a growing concern that if the market did not control this realm, the government would intervene (S. Gupta 2018). Large corporations with significant influence and bargaining power started influencing the market (C. Gupta 2017) using a variety of methods, such as issuing mandates for its vendors to provide certain privacy controls (Nehf 2005) or publicly pledging to transparency around emerging technology (National Telecommunications and Information Administration 2018). As Gupta found when evaluating the privacy drivers in the marketplace, when a single actor can affect change that "results in tangible and visible benefits to consumers, who can then question why other actors in that space are not implementing it" (C. Gupta 2017, 761), that single actor changes the marketing game. Their competitors, who do not offer the same visible benefits, face loss of reputation along with market share (C. Gupta 2017).

Lastly, it is relatively easy for entities to post a privacy statement online that discloses their actions towards personal data, however immaterial the statement may be and further, the law applicable to such a market or activity may require a notice to be posted. Consumers expect to see an online privacy statement when they do search for one and at least one state, California, requires an online privacy statement to be posted, notwithstanding the CCPA. Also, if an entity is found to violate its public statements, the FTC may seek enforcement under Section 5 for unfair and deceptive trade practices, where the entity is subject to FTC oversight. Out of the eighty-two laws where the FTC has jurisdiction, there are quite a few likely to apply to Universities (see (U.S. Federal Trade Commission 2021)Federal Trade Commission 2021). What an entity says it does or does not do with personal data reflected in its publicly posted privacy notice, if not true, can be held against the institution as an unfair or deceptive trade practice.

Given the clear direction of for-profit entities and market practices towards using privacy as a market differentiator, it seems a natural progression for universities to consider the same when competing for consumers. There are only a finite number of individuals entering institutions annually and each university wants to entice as many as possible to its campus. At the same time, states are decreasing the funds allocated to public institutions (Mitchell, Leachman, and Masterson 2017). States must compensate for the decreased funding by increasing enrollment and tuition while searching for other sources of funding, such as grants – each of which rely on the university being attractive to the target populations. Hence, marketing. Universities market by academic departments, sports, scholarship, awards, and innovation (see e.g., (U.S. News and World Report 2021). All the above considered, it is a greater possibility that

experiencing a personal data breach is more likely to impact a university's move towards privacy.

Once a university increases its data protection, it is possible to use that as a market differentiator or, as in the corporate examples above, once the new protections are visible to the consumer, the consumers expect all comparable offerings to have the same level of information security controls. Marketing efforts by public entities around privacy have already begun. One example blends the two aspects – the entity's own privacy controls and privacy offerings to the public. In 2017, the U.S. Army conducted a recruiting campaign for civilian hackers (Lockie 2017). Out of 9.8 million viewers, 800,000 took the challenge. One percent passed.

2.5 Chapter 2 Summary

Review of the literature demonstrates that this is a topic ripe for review. In the U.S., states are passing omnibus privacy laws, exchange of data with other nations is at risk, and the prevalence of laws applicable to Universities is growing. Universities collect and use an enormous amount of personal data and given the level of complexity in the institutions and in the law, privacy compliance at Universities is growing even more complex as it compounds. Implementing privacy programs or re–designing current programs to align with a growing body or policies is difficult and history has not shown Universities to undertake such efforts easily.

CHAPTER 3

DELPHI METHOD

3.1 Introduction to Delphi Method

The selected research approach utilized a Delphi method, a qualitative approach facilitating data collection using a series of questionnaires to gain consensus. The Delphi method traditionally requires a collaborative process whereby an expert panel (Experts) engages directly to address the issue presented to them. This was an appropriate qualitative approach for this research question given the objective to identify how Universities in the United States are managing compliance with privacy and data protection laws. The experts were not being engaged to solve a problem, but rather to identify the factors that should be assessed given the multifaceted complexity of the subject matter. Privacy management and compliance is a broad and relatively untried field with innumerable facts, applications, and unsettled law. Rowe and Wright (1999) define a classic Delphi method by four characteristics: anonymity, iteration, controlled feedback, and statistical aggregation of the group response. Scholars are divided on the structure of a Delphi, with some opining only Delphi studies that meet this criteria are legitimate, while others believe that the method can and should be modified as needed to meet the requirements and intent of the studies (Skulmoski, Hartman, and Krahn 2007).

The intent of using the Delphi method in this study was to reach consensus among privacy experts as to the critical factors to examine when assessing whether Universities are subject to and compliant with various privacy laws or standards. The concern was how to narrow the scope in an objective manner to increase the academic rigor, thereby reducing

researcher bias. Using the Delphi method in this manner accomplished the goal by determining the elements of privacy compliance critical to a study of this nature.

The design of the Delphi method needed to accommodate both conducting research during a global pandemic and protecting the confidentiality of the respondents (a concern among privacy professionals). A modified technique was applied using a series of three online surveys issued via anonymous survey links. Each survey successively builds on the one before, leaving the results of the third survey representing the consensus of the participants. A midsized participant pool was appropriate for the qualitative approach as participation was expected to decrease from one Delphi round to the next. Round one used an open-ended questionnaire to gain as much information as possible for the study (Skulmoski, Hartman, and Krahn 2007). Please see Figure 5 for a visual of the Delphi

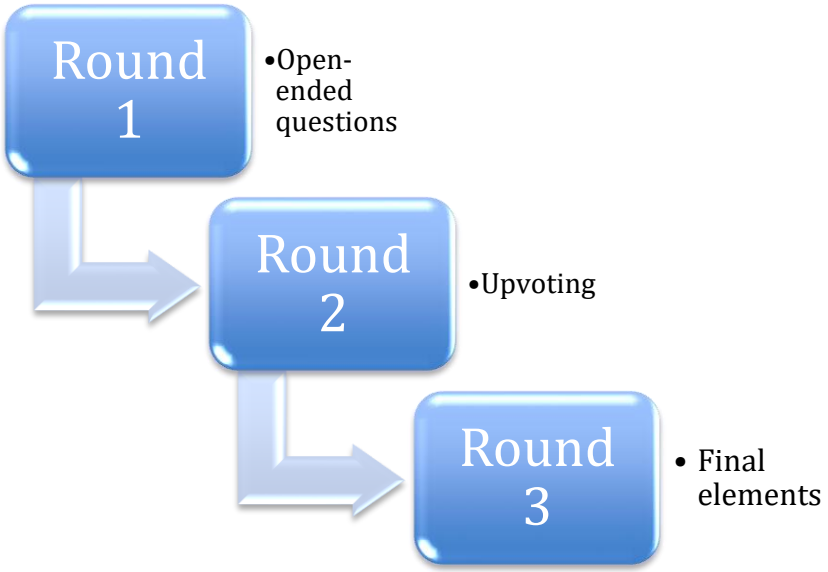


Figure 5: Delphi Process

process. The information was collected, analyzed, and themed before questions for subsequent rounds were developed. The Delphi method consisted of three rounds but remained flexible to allow for additional rounds if a consensus had not been reached. The design required question revision and resubmission to the Institutional Review Board after each round, which allowed collection of meaningful data which could lead to a deeper understanding (Okoli and Pawlowski 2004).

3.2 Expert Panel Participants

As noted above, the design requires a panel of expert participants who are familiar with privacy laws that apply to Universities. Two major factors drove the panel design: the broad scope of law applicable to Universities and the small number of privacy professionals at Universities. Actual experience in managing privacy at Universities was not as critical as having enough qualified privacy professionals participate, although the University experience was one of the demographic questions.

The goal was to recruit from a pool of professionals with experience in privacy ranging from less than five years to over twenty-five years – weighing heavily towards most Experts having fifteen years or more of privacy experience in a variety of contexts. Experts were recruited via electronic communications, either email or social media messaging. Ideally, Delphi groups should have the appropriate number of participants to achieve the goals and given the modified format, the number also needed to account for anticipated attrition from Round one to Round 3. Delphi studies have varied greatly in number of participants (Skulmoski, Hartman, and Krahn 2007), with the emphasis on the circumstances and question(s) while accounting for attrition (Bataller-Grau et al. 2019). Although the

number varied greatly, the ideal number to accomplish the purpose ranged between fifteen to thirty. Thus, the goal for this research was twenty Experts per round. The nature of the design, however, removed the ability to track participants across rounds, but offered heightened confidentiality.

The Experts in the Delphi are not a sampling of a population, they are the population (Fink et al. 1984; Skulmoski, Hartman, and Krahn 2007). Therefore, "a purposive sample is necessary where people are selected not to represent the general population, rather their expert ability to answer the research questions" (Skulmoski, Hartman, and Krahn 2007, 4). Once an initial group of experts is identified, a "snowball" sampling can then be used to generate subsequent participants (Hartman and Baldwin 1995; Mason 1996). In this instance, purposive sampling, a form of non–probability sample which is also known as selective or subjective sampling, was used. In purposive sampling, researchers rely on their own judgment when selecting the members of the population to participate in their surveys. This method requires the researcher to choose and approach eligible participants based on the particulars and goals of the individual study. All participants must fit the profile of people who should be involved in the study. Often this seems like a convenience sample, but it is not, and it is not an interchangeable term (Skulmoski, Hartman, and Krahn 2007). The population needed here was experienced privacy professionals with knowledge of the various privacy laws that could apply to Universities and understand how and why those laws might apply.

Except for FERPA, privacy professionals at Universities manage the same privacy laws, triggers, compliance requirements, and enforcement penalties as privacy professionals do at private companies. This made for a broad population pool. The qualifications for

Experts are "i) knowledge and experience with the issues under investigation; ii) capacity and willingness to participate; iii) sufficient time to participate in the Delphi; and iv) effective communication skills" (Skulmoski, Hartman, and Krahn 2007, 10). Therefore, the goal was to recruit privacy professionals who could speak to a wide range of privacy requirements and are familiar with laws that are potentially applicable to Universities. FERPA specifically governs educational privacy, but the remaining applicable laws are either sector-agnostic or activity-specific. In addition, given the extraterritorial application of key data protection laws, the study needed the input from professionals experienced in privacy laws around the world, albeit with a focused intent to recruit heavily from the U.S. rather than a non–U.S. pool. Therefore, the goal was also to recruit Experts with a global span of experience.

The recruitment and resulting expert panel are critical to the strength of the results. First, the parameters for participation were determined in advance, accounting for the significant increase in the number of privacy professionals in the past few years.[7] The intended goal was to have a panel comprising half privacy professionals with fifteen years or more of experience in privacy, another 45% with between five to fourteen years of experience, and the last few saved for privacy professionals with less than five years of experience. The goal for geographical location was a simple majority of U.S. professionals versus non–U.S. professionals. There were no set parameters for Experts with direct experience in privacy at Universities, just an intent to

[7] In 2009, the International Association of Privacy Professionals (IAPP) had 5,000 members globally which grew by 50% in 24 months to 7500 at the end of 2010 (Roman 2011). In 2015, the IAPP had 25,000 members. In 2020, it had 65,000 members. Previously, with GDPR entering into effect in 2018, the IAPP estimated in 2017 that 75,000 new privacy professionals would be needed. In 2019, a study showed that over 500,000 companies registered data protection officers. Data Protection Officers are a required role based on the types or amount of data processing activity by a company. Data Protection Officer (DPOs) are very similar to Chief Privacy Officers (CPOs) in the level of knowledge, skill, and expertise required.

recruit Experts with such experience. This was due to both the small number of privacy professionals at Universities and the potential that current privacy professionals at Universities would be reluctant to divulge potential non-compliance issues. The researcher approached noted professionals in the privacy field ranging from key figures in academia, industry association groups, think tanks, law firms with a specialty arm in privacy, privacy consulting companies, and Fortune 500 companies. Referrals, in the snowball sampling caliber, were sought from professionals at Universities, industry associations, and think tanks – with minimal results.

The goal was to have 20–30 participants, therefore the number invited tripled to account for declines and attrition. In the end, 94 professionals were invited to participate. Of those invited, 57 agreed to participate, 37 did not respond, and none declined. Participation surveys were only sent to the 57 who explicitly agreed to participate via the recruitment process.

The Resulting Panel

Of the resulting 57 acceptances, forty of them are lawyers working in the privacy field (see

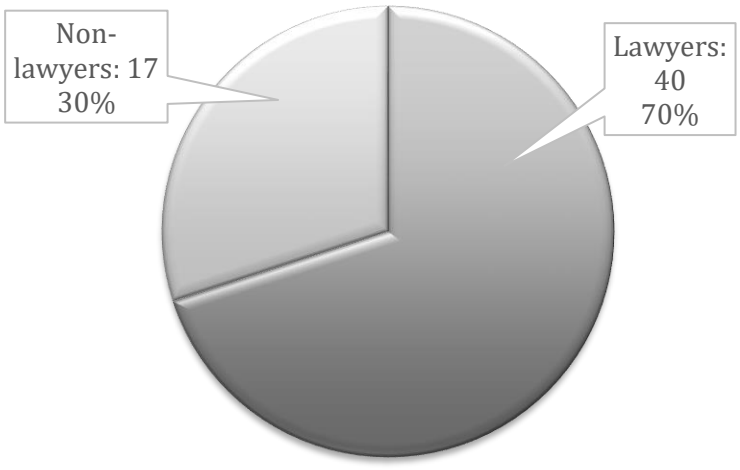


Figure 6: Visualization of Experts' Professions

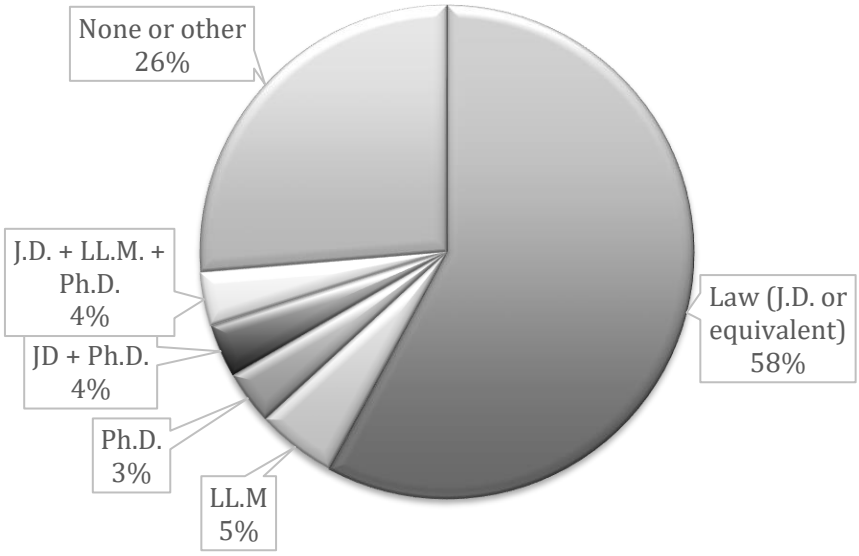


Figure 7: Advanced Degree Type

Figure 6), two of which also have PhDs, three have advanced law degrees (LL.M), and two have all three – a law degree, an advanced law degree, and a PhD (see Figure 7). Two additional Experts have PhDs. All but seven have a global span of coverage as seen in **Figure 8**.

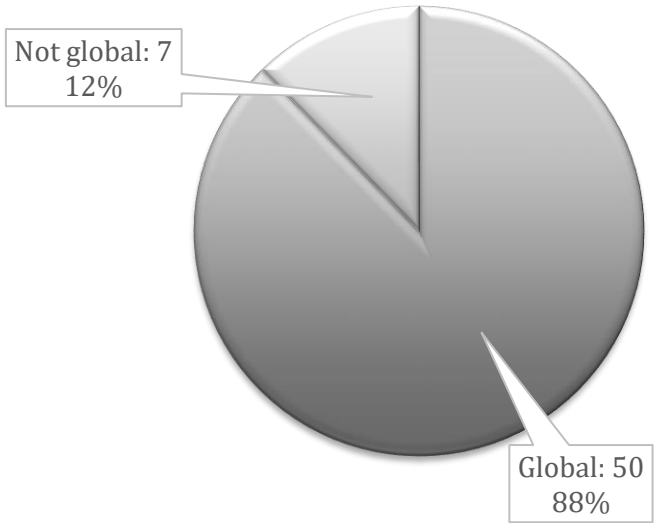


Figure 8: Global Span of Coverage

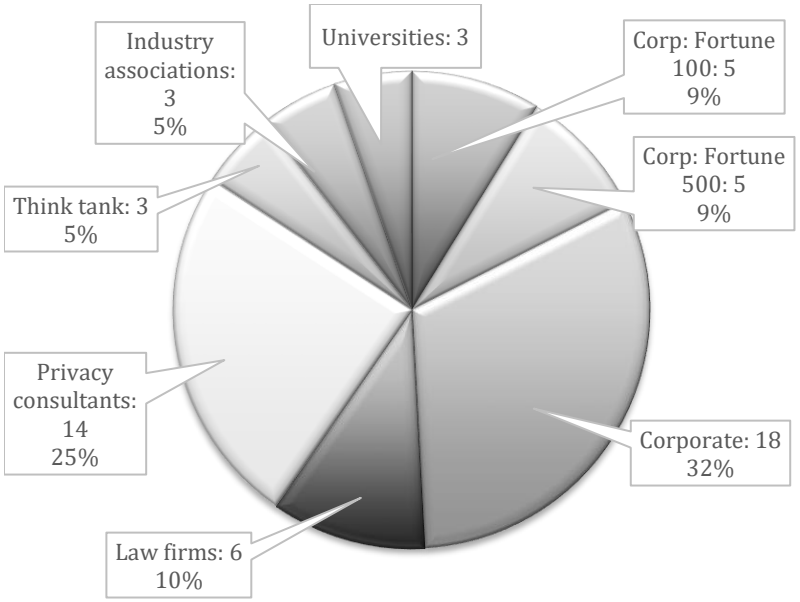


Figure 9: Work Environment

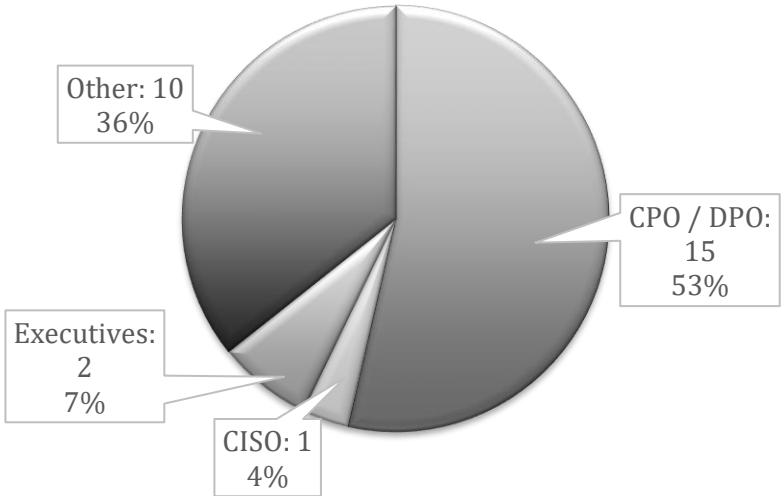


Figure 10: In-house Roles out of 28 Experts

Five are from Fortune 500 companies and an equal number from Fortune 100 companies. Six are at law firms, either global law firms with a dedicated privacy practice or a boutique law firm. Fourteen are consultants, specializing in privacy. There are three each at think tanks, industry associations, and universities. **Error! Reference source not found.** shows the scope of the

Experts' work environments. Of the twenty-eight working in-house at companies, fifteen hold CPO or Data Protection Officer (DPO) roles, one is a chief information security officer, and two are executives at start-up tech companies specializing in information management (see Figure 10). Two Experts are considered preeminent scholars in privacy. At least ten Experts also work in cybersecurity. At least forty-five are also adjunct professors teaching privacy or privacy-related courses. Please see

Figure 11 for their additional experience. In addition, the past or concurrent experiences of these Experts include senior government roles, significant privacy scholarship, noted speakers, and appointed representatives to local and global boards and committees. Forty are certified in privacy, with thirty-two having multiple certifications. Certifications are shown in Figure 12.

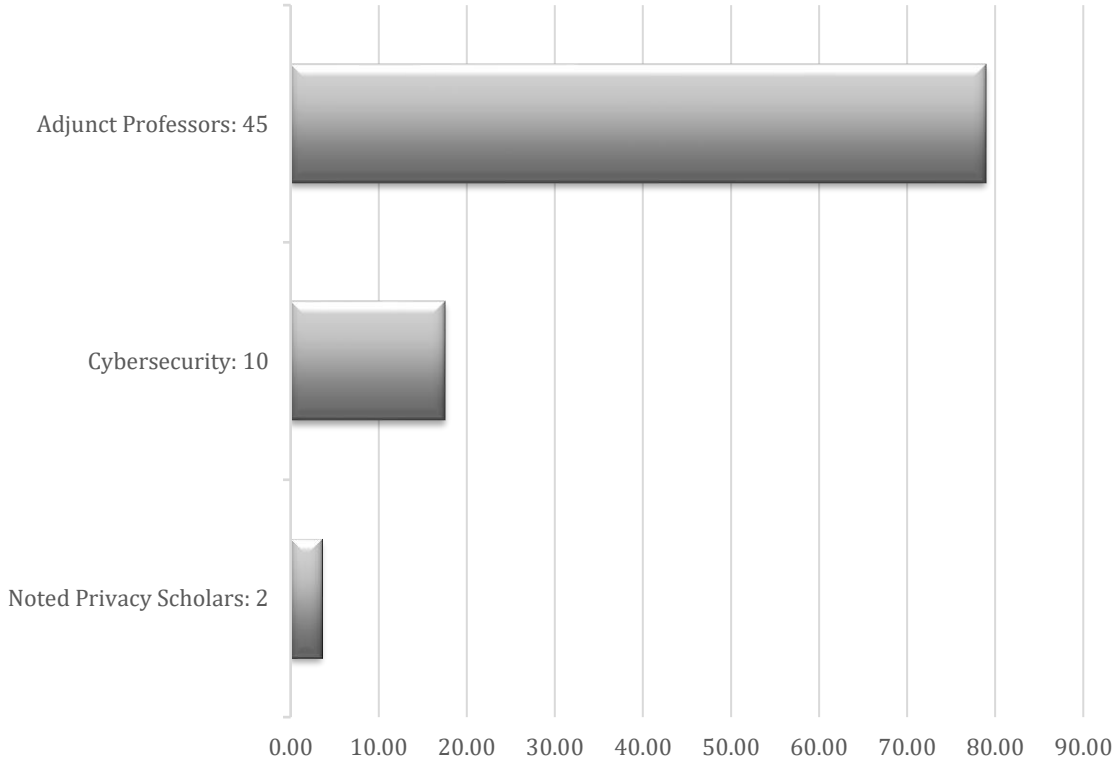


Figure 11: Additional Experience

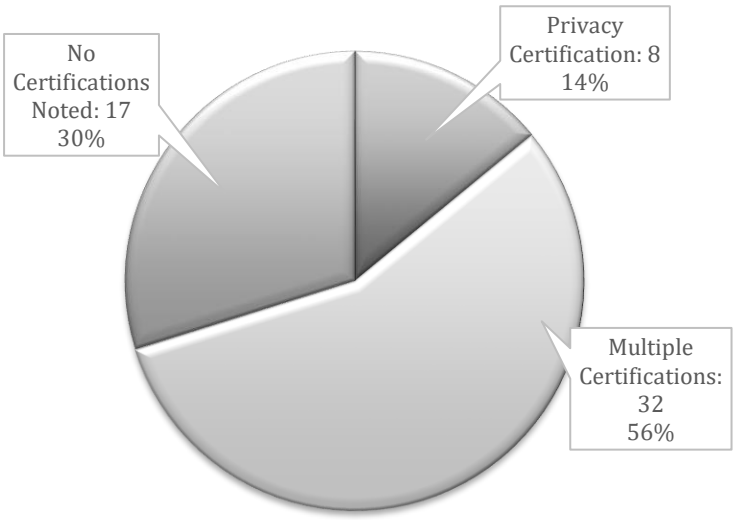


Figure 12: Certifications

Given the measures to ensure anonymity of the actual responses, it is not possible to provide a detailed analysis of those who responded per round. However, Table 3 provides the number of Experts who participated per round broken out by the years of experience. In the less than five years' category, only four Experts participated and all in Round 2. In Round 1, eighteen Experts had more than fourteen years of experience while ten had between five and fourteen. In Round 2, the division changed with the previously mentioned four with less than five years of experience, twelve in the middle range, and eight with fifteen years or more of experience. In the last round, the majority of the Experts were in the higher experience category while thirteen were in the five to fourteen years.

Table 3: Number of Experts per Round

Years of experience in Privacy	**Round 1**	**Round 2**	**Round 3**
< 5 years	0	4	0
5–14 years	10	12	13
>14 years	18	8	17
Totals	**28**	**24**	**30**

Rounds 2 and 3 were sent to the same fifty-seven Experts as those who received Round 1. No one requested to be removed from the subsequent study questionnaires.

At a minimum, thirty-five unique Experts participated in at least one round. This is calculated by adding the highest number of respondents in each experience bracket (< 5, 5–14, >14) respectively four, thirteen, and eighteen. At a maximum, fifty-seven Experts participated in total, although not all fifty-seven in any one round, much less all three rounds. The results of all three rounds are provided below.

3.2 Research Engagement

Questions

The objective of the modified Delphi method was to reach consensus on factors to consider in assessing privacy management at Universities and to ultimately, provide insight to University leadership in general and to University privacy professionals specifically towards maturing the privacy compliance landscape at Universities. The following research questions were used:

Q1: Is managing privacy compliance at Universities a complex engagement?

Q2: What privacy laws or regulations are Universities subject to?

Q3: What factors at Universities trigger privacy laws?

Q4: What characteristics of Universities influence privacy compliance?

Each of these questions required several sub-questions to delve into the nuances of the inquiry.

Instrumentation

In this phase, the research instrumentation for collecting data comprised the Delphi method and three rounds of electronic surveys, issued via Qualtrics using the "anonymous mode."

Round 1

The Delphi Round 1 instrument included a mix of demographic questions and open-ended questions, intended to elicit comprehensive responses without directing the content or leading a response. The demographic questions were repeated for each round. Each round was submitted to the IRB for approval prior to being issued.

Round 2

Once the responses were received and the survey closed, the responses were analyzed and grouped into categories based on the responses. The open-ended nature of the questions resulted in a variety of responses that were unquantifiable, although they provided insight into the extent of the problem Universities face. More information is provided on this observation below in results. Round 2 was then submitted to the Institutional Review Board for approval and subsequently issued to the expert participants.

Round 3

Once the responses from Round 2 were received and the survey closed, the responses were tallied and used to create the Round 3 instrument. The analysis of Round 2 and subsequently, Round 3 were much faster because the available responses were listed within each category and the participants were asked to select a certain number out of the pool of possibilities. This functioned as a short series of upvoting to narrow the pool to those responses that

received the most votes. Once the Institutional Review Board approved Round 3, the survey was issued to the Experts.

Consent, Confidentiality, and Data Retention

Before individuals participated in research, they were informed of the purpose of the study, what data will be collected, the risks involved in participating, and how the results will be used. Transparency and consent are both foundational principles of privacy and integral to conducting research with human participants (Rhodes 2010). Each round of surveys included an informed consent form, see Appendix E, as the first page of the survey. Experts could not advance past that page without consenting. To withdraw consent, Experts could cease answering and / or not submit their responses. Individuals could also communicate their desire to withdraw to me or the chair of my dissertation committee, who was also prominently listed as a contact for the study.

In research, one primary way to reduce risk to participants is not to disclose their identities. Research privacy is vital to social sciences and ethical codes in humanities (Surmiak 2018). Even in a low-risk study such as this one, the assurance of confidentiality reduces anxiety for participants and can lead to more openness.

For confidentiality, several steps were taken. The names of the participants will not be released, and the surveys were not linked to individual respondents. The surveys were designed and issued through Qualtrics using the "anonymous" link functionality. All respondents received the same link and there is no re–identification key maintained. The demographics will be used to illustrate the expertise of the panel, but will not be associated

with respondent identifiers, such as email address or names—the latter of which are not collected in the survey process itself.

On the positive side, taking this approach assured maximum confidentiality, near anonymity. On the negative side, it means that there was no insight into which of the respondent pool of those who agreed to participate actually did respond, thus, no means to send individual reminders. In addition, respondents could not be directly tracked to identify who answered any, two, or all three surveys. Indirectly, the demographic information could be used as a key across rounds to attempt to identify those who continued to be involved, verify participation across rounds and address attrition. However, once downloaded, the demographics were divorced from the responses. Given that this is a research study about privacy, to privacy professionals, from a privacy professional, and the failure of the initial study due to essentially privacy concerns, this inability to track Experts across rounds is not considered a weakness in the overall results.

Although the overall research was not anonymous, there was no avenue to certify that only the researcher would have access to the key to re–identify respondents or that the key or identifiers were destroyed, because no key was generated. No numerical codes were assigned. This maintained an even higher level of protection for the Experts.

In addition, the data will be retained for three years in an online file storage system that has security controls in place for encryption and access management. Once the retention timeframe has passed and the purpose for the data collection no longer exists, the data will be irretrievably destroyed. Retention, destruction, and purpose limitation are all fundamental privacy concepts as well.

Collection and Analysis Process

As provided above, the Experts were approached in advance to recruit them for the study. No one refused, although the demographics revealed that at least one response was not from a recruited respondent (discussed in more detail in the results portion).

Once each round was approved by the Institutional Review Board (IRB), respondents were sent a message via email or other online messaging platform, see Appendix F. The message contained basic instructions and a link to the survey instrument. Respondents did not receive reminders given the confidentiality provisions within the study prohibited identification of responses. The second and third rounds were not open-ended questions, with one exception as noted below in Round 3. Respondents were asked to select a certain number of items from each question as indication of what they opined were the most important or impactful items from the entries provided across all respondents. Opportunity was provided for commentary within the instrument.

Round 1 comprised mostly open-ended questions aside from the informed consent and demographics. Content analysis, drawn from the researcher's unique insider perspective, was performed to both eliminate non–responsive or non–specific items and then to group similar responses. Microsoft Excel and Qualtrics analytics were used for review and analysis. demographic information was segregated for separate review unrelated to the content analysis. Rounds 2 and 3 were reviewed using Qualtrics analytics downloaded into Microsoft Excel. Demographic information was divorced from the substantive questions. Comments were reviewed, if received, for impact to responses. There were no comments that impacted substantive responses.

The results of the Delphi Method were then used to inform the content analysis of publicly available resources from the selected Universities and used to help narrow the Doctrinal Legal Research portion. This was an acceptable process that focused the research to those factors deemed most relevant in assessing whether Universities are subject to privacy laws and if so, how Universities are managing privacy compliance given the complex nature of both Universities and privacy.

3.3 Delphi Method Results

The basic design of a Delphi eliminates the in-person dynamics where accuracy and knowledge may be overwhelmed by voice or presence (Avella 2016). By using electronic means to collect responses, the Experts have no insight into who provides what input, thus avoiding potentially problematic dynamics. Even with a field of Experts like that gathered in this study, there are still those who will always hold more influence by the nature of their experience and authority or their force of will. Using the online survey instrument eliminated undue influences and let the results and process speak for itself. The sections below detail the results.

3.4 Results of Common Demographic Questions Across All Rounds

There were four demographic questions presented across all three rounds. These responses were divorced from the substantive questions to better enforce anonymity of the responses. The first question was about where the Expert was located, either within the U.S. or outside the U.S. The results of this question across the three rounds are presented in **Error! Reference source not found.**, followed by a visual depiction in Figure 13. Those participating from non–U.S. locations comprised sixteen percent or less of each round.

Table 4: Location of Experts: U.S. / Non–U.S. Per Round

	Round 1	Round 2	Round 3
Location: U.S.	22	21	25
Outside the U.S.	4	4	3

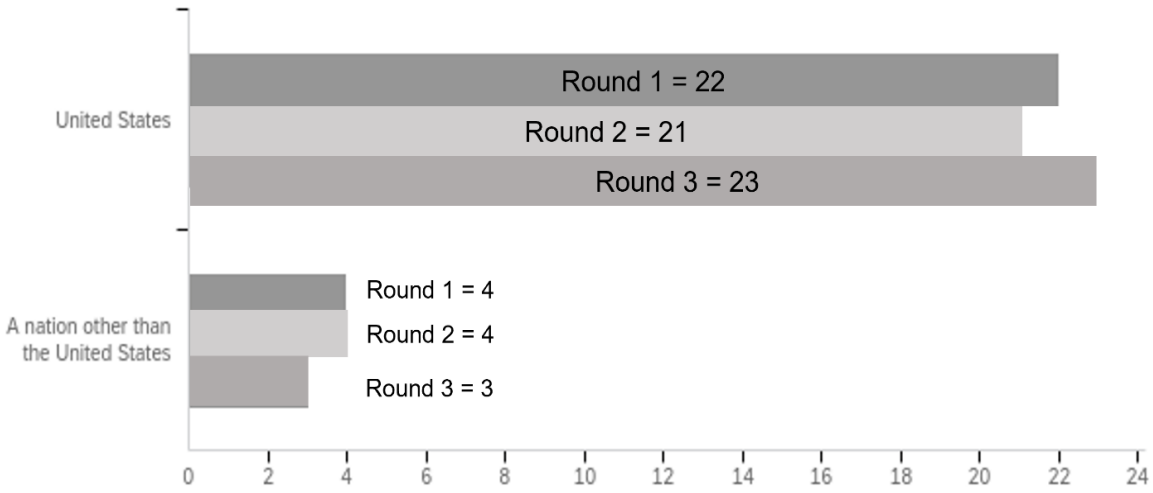


Figure 13: Geographic Scope Across Rounds

The next three questions centered on the respondent's expertise in privacy. The first two were given in five-point ratings where one star meant the person had little knowledge or experience and of U.S. five stars meant the person was very comfortable in their knowledge in that area. The first question was on their experience in privacy law in the U.S. and the second was on managing privacy laws at Universities. The third question was a text entry that asked for their years of experience in privacy.

The results of these questions across the three rounds are presented below in Table 5. In each round, the self-rated level of experience in privacy was highly skewed to five stars. Experience in managing privacy at universities was more evenly distributed, although Round 2

did weigh heavier in the lack of experience. However, the years of experience in the first and last round met the parameters of including more than half the Experts at fifteen years or more of experience, although they lacked any input from Experts with less than five years of experience. Round 2 deviated from this goal with 50% with 5–14 years of experience, 33% with more than fifteen years of experience in privacy, and 17% with less than five years of experience.

Table 5: Privacy Experience Across Rounds

	Privacy Experience 1–5 stars					**University Privacy Experience 1–5 stars**					**Years of Privacy Experience**		
	1	2	3	4	5	1	2	3	4	5	< 5	5–14	>14
Round 1	0	0	2	4	20	5	2	4	7	8	0	10	16
Round 2	0	2	3	7	12	10	2	2	5	5	4	12	8
Round 3	0	1	2	5	20	8	2	6	3	9	0	13	15

Although the results of numbers of years of privacy experience are broken into the three ranges, the Experts provided pure numerical responses. Thus, there is more detailed experience on the exact years of experience for each Expert. In Round 1, there were three Experts with twenty years of experience and seven with more than twenty years. The highest number was twenty-six years. In Round 2, five Experts had twenty years or more experience; two of which had twenty-five years of privacy experience In Round 3, seven Experts had twenty years or more of experience with three having twenty-five years.

3.5 Round 1

In the first round, the goal was to ask open-ended questions to drive the options for the two subsequent rounds. In Round 1, there were three questions that were not used in subsequent rounds. They are substantive questions but intended to gain initial insight into the management

of privacy Universities. Although close-ended only permitting a yes or no response, each question permitted optional comments. The first question asked whether the Experts believe that achieving privacy compliance at universities is simple or complex. The second was whether the Experts believe that achieving privacy compliance at universities is simple or complex. The last question was whether the Experts believe that most universities are effective at managing / achieving privacy compliance.

The last part of the Round 1 questions elicited open-text responses that would be aggregated and "voted" on in the two subsequent rounds in order to have the Experts narrow to the topics to focus on in this study. There were five open-text questions for Experts to identify the types of data subjects and then the types of activities present at universities that would trigger privacy laws; the privacy laws / requirements that are important for universities to follow; the programmatic elements that should be present in a University privacy compliance program; and the risk factors at universities for non–compliance in terms of privacy compliance. Once the responses were received, they were tallied and sorted for commonalities. Question 5 in the last section showed complexities in how the question was interpreted (for consequences or risks rather than risk factors), discussed in more detail below, that an in-person session may have prevented, but nonetheless, the process continued. The full responses of the insight questions and the substantive questions for Round 1 are in Appendix G.

Round 1 Responses

The survey was open from February 6 – 26, 2021. Thirty-eight Experts started the assessment, eleven did not complete the assessment. One respondent was disqualified when the response to years of privacy experience indicated one year of experience. The respondent sent an unsolicited

communication explaining that the invited Expert assigned the questionnaire to an intern to complete. This was outside the parameters of the study and subsequent instructions emphasized the integrity of the assessment relies on the expertise of the invited participants. The incomplete and disqualified responses were deleted from the dataset. This resulted in a total of twenty-six respondents, meeting the desired number of at least twenty Experts. The results of the demographic questions are presented above. Below are the results of the insight questions, whether privacy compliance is simple or complex and whether universities are effective at achieving compliance. Each question had fifteen comments submitted. Figures 14 and 15 represent the responses, respectively, with the comments from each one presented further below in Tables 6 and 7.

Round One Insight Questions

The first insight question was "Do you believe that achieving privacy compliance at universities is simple or complex?" As seen in Figure 14, all responses indicate that privacy compliance at

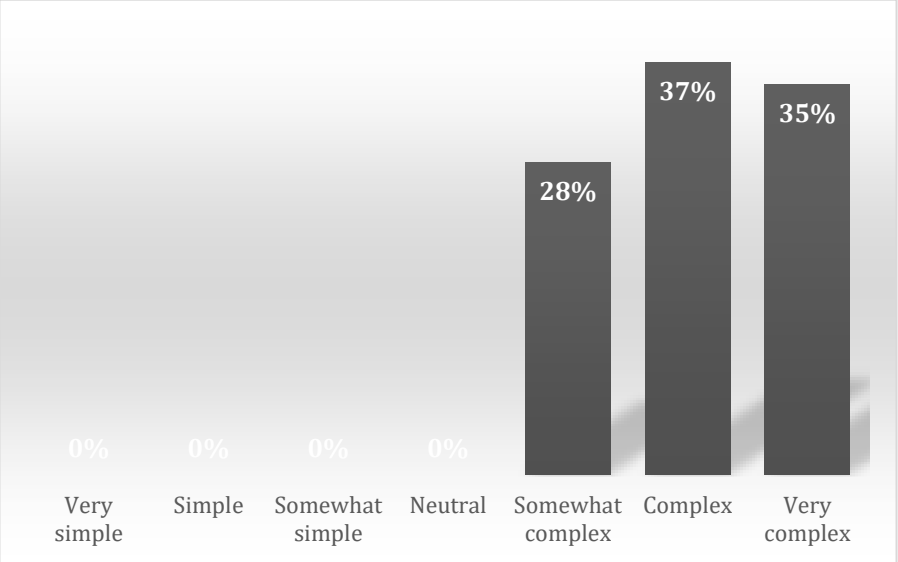


Figure 14: Complexity Level

Universities is complex at some level, with most of the Experts opining that it is complex at 37%, followed by very complex at 35%, and somewhat complex at 28%. No one responded as neutral or any level of simple.

Table 6: Comments on Complexity of Privacy Compliance at Universities

1	Colleges and Universities can be extremely siloed entities with internal stakeholders who don't generally focus on broader compliance and risk factors of the data they have access to - including "people data."
2	diverse stakeholders w/different expectations of privacy
3	Handling student data is not extremely complex. This complexity goes up due to Covid (health info), remote learning. Most complex: Handling and sharing of research data that contains personal data.
4	highly complicated entities subject to a broad variety of laws
5	It goes beyond FERPA, which is where most stop.
6	So many data sources; different goals for the data; competing priorities (protection vs. wanting to use certain data for research, planning, etc.)
7	The open nature of universities makes the concept of privacy especially challenging.
8	The diverse nature of the parties for which you are protecting as well as the nature of resource allocation makes it more challenging than in a corporate setting. This being said, universities that have been subject to breaches and fines are often penalized or fined less. This should not be so if we wish to force improvements. As non-profits, most larger universities have immense endowments and budgets yet focus more on athletic and senior leader spending to their detriment. They are also often inflexible in regard to contracts and other legal arrangements, however again they often do not have the resources to invest in in-house legal teams with the sophistication to be able to merit this inflexibility.
9	Universities are inherently about collaboration and sharing information. They are inherently innovative, employing new technologies, and pushing social norms. In that context, finding the right place and approach for privacy compliance is a difficult (and always moving) target.
10	The difficulty of privacy correlates with the amount of data. Universities obtain large amounts of data about and from individuals. Additionally, universities are a big target for data compromise.
11	The complexity comes with the ages and variety of people and information that a university holds about people.
12	Risk management based, so difficult decisions and technology legacy leads to complexity
13	International data transfers; application of different state laws; expansion of universities into nontraditional areas
14	Universities are particularly challenged by the academic freedom required by professors and other researchers to properly protect any information they collect, irrespective of whether it is personal information. Having personal information is just one facet of that.
15	Universities are very decentralized; it's difficult to have all schools and departments implement the same policy, even if it is adopted centrally

Fifteen comments were provided, as presented in Table 6. The comments reiterate what was found in the literature review, that privacy compliance is not a simple undertaking and that universities manage quite a bit of data in various activities that implicate more than just FERPA. The comments were widely diverse, with one unifying theme—privacy at Universities is complex and intelligent minds focus on varying aspects of privacy. Several comments spoke to the complex nature of Universities, while others spoke to the scope of the data being managed. One Expert opined that "[h]andling student data is not extremely complex. This complexity goes up due to Covid (health info), remote learning." "Universities are particularly challenged," writes another Expert, "by the academic freedom required by professors and other researchers to properly protect any information they collect, irrespective of whether it is personal information. Having personal information is just one facet of that."

The second insight question was "Do you believe that most universities are effective at managing / achieving privacy compliance?" As seen in Figure 15, 38% feel that Universities are somewhat effective in managing privacy compliance, while the next largest group was neutral—neutral being the option between the ranges of effective or ineffective. The next largest percentage of responses fell in the somewhat ineffective range at 19%. This results in 80% of Experts falling into the middle of the options between somewhat effective to somewhat ineffective. Only 4% felt that Universities were effective at this effort but offset by an equal amount of those who felt Universities were somewhat effective in managing privacy compliance, while the next largest group was neutral— neutral being the option between the ranges of effective or ineffective. The next largest percentage of responses fell in the somewhat ineffective range at 19%. This results in 80% of Experts falling into the middle of the options between

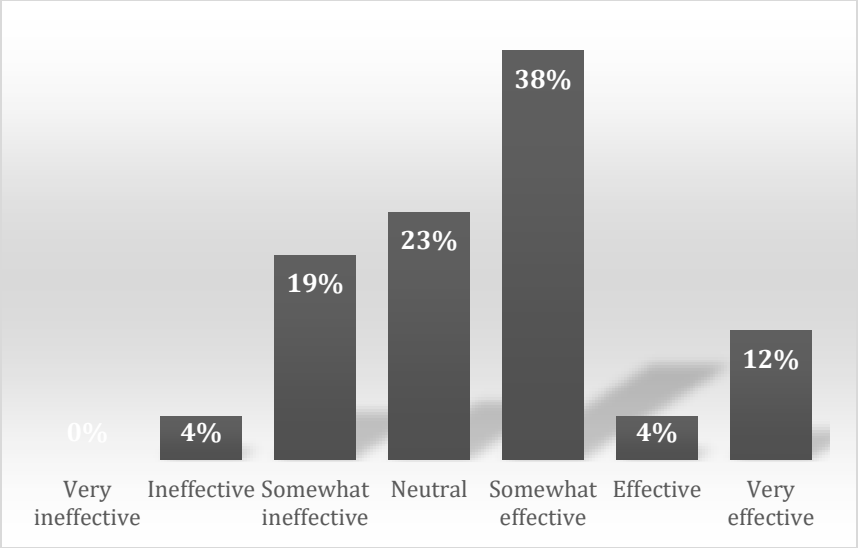


Figure 15: University Effectiveness at Managing / Achieving Compliance

somewhat effective to somewhat ineffective. Only 4% felt that Universities were effective at this effort but offset by an equal amount felt they were ineffective. No one felt Universities were very effective at managing privacy compliance, but 12%, the fourth highest range, feel that Universities are very ineffective at managing or achieving privacy compliance.

Fifteen comments were also provided on this question, as presented in 7. These comments were also quite diverse ranging from speaking to the complexity of managing privacy laws, to the issues of privacy siloes or areas of privacy to those who hold positions in universities. One respondent commented with a link to an Educause poll related to the topic.

Table 7: Comments on Effective Management of Privacy at Universities

1	And my experience with universities related to privacy has to do with consent-based background checks that include degree verification and education history information. I dealt with many different schools of different sizes in different states, and all seemed to be fairly knowledgeable of the requirements needed in order for our teams to obtain information about current or former students. However, most outsourced These activities and when you got directly in touch with the University the knowledge and level of compliance did change (not as good/organized/consistent).
2	Data Privacy is mostly a "check-the-box" compliance exercise.
3	For the size of target they do a pretty good job, I believe.

Table 7, continued.

4	I don't believe it is something government entities excel at.
5	Universities are inherently about collaboration and sharing information. They are inherently innovative, employing new technologies, and pushing social norms. In that context, finding the right place and approach for privacy compliance is a difficult (and always moving) target.
6	In terms of pure compliance, they're mostly fine. But there are lots of privacy problems in the university. Universities only have so much direct control over their ecosystem, especially in the COVID era - things like LMS and lockdown browsers are super problematic and also difficult to control by the university directly.
7	There are many dimensions to privacy
8	I don't have information to inform my response.
9	I really don't know. Most university CPOs I know (not professors) are no longer at that job.
10	FERPA compliance probably addressed well. Evolving regulations like CCPA/CRPA unclear on how Universities might comply with sharing datasets collected for Artificial Intelligence or Machine Learning research
11	It depends on what you mean by "achieving privacy compliance. Most seem to make a sincere effort, but sometimes it's a "check the box" approach to FERPA, sometimes it's more thoughtful and comprehensive. But neither one is fully "achievable" in the complex university environment.
12	My experience is limited to university systems that have research or hospital structures as I am focused on the life sciences. I am also knowledgeable about publicly disclosed breaches and fines. Most often I have seen staff, including doctors/scientists, who believe they and their university are infallible and legal teams that are not as experienced as they need to be when dealing with their corporate counterparts.
13	Ref - https://er.educause.edu/blogs/2020/11/educause-quickpoll-results-risk-privacy-and-compliance
14	Very complex compliance landscape; lack of desire (perceived ROI) to invest in privacy
15	Legacy of lack of centralised data management

Educause is "a nonprofit association and the largest community of technology, academic, industry, and campus leaders advancing higher education through the use of IT" (Educause 2021) and is the resource for much information on privacy in education. One Expert provided context for his / her response:

> And my experience with universities related to privacy has to do with consent-based background checks that include degree verification and education history information. I dealt with many different schools of different sizes in different states, and all seemed to be fairly knowledgeable of the requirements needed in order for our teams to obtain information about current or former

students. However, most outsourced these activities and when you got directly in touch with the University the knowledge and level of compliance did change (not as good/organized/consistent). Another opined on the nature of Universities and their privacy "Universities are inherently about collaboration and sharing information. They are inherently innovative, employing new technologies, and pushing social norms. In that context, finding the right place and approach for privacy compliance is a difficult (and always moving) target." Several others spoke up about privacy being a check-the-box exercise. And others reinforced the complex environment of Universities.

Substantive questions (open response in Round 1)

Each set of responses in this section were individually sorted alphabetically to further divorce responses. Where necessary, cross-references were substituted with the referenced language. Below, commonalities were identified amongst the responses, which is also the process used to drive the itemized list in Round 2. Where indicated, notable responses are provided. However, the first question below on the types of data subjects that would trigger privacy laws was not included in the substantive upvoting rounds. This was because the types of data subjects are relatively ubiquitous at most Universities. Certainly, all Universities must have students, staff, family, visitors, alumni, members of the public, payors, and people with disabilities. There are some data subjects which might not be present at all Universities, and these will be sorted out and included in the Document Analysis without additional up voting necessary.

For the first question on what types of data subjects present at universities would trigger privacy laws, the responses were grouped into fifteen categories. The majority of categories had subcategories, such as students could be subcategorized into applicants, minors, exchange students, and student athletes. These fifteen categories are: students, staff, families, visitors, patients, vendors, research subjects, customers, alumni, donors, faculty, members of the public,

payors of student fees, locale-based individuals, and people with disabilities. In many categories, there are multiple subcategories that have been grouped into a main category. “Students” include applicants, minors, exchange students, and student athletes. “Staff” includes employees, contractors, applicants, directors, and regents. “Families” include parents and dependents. “Visitors” include guest speakers. “Vendors” include vendor personnel and service providers. “Faculty” includes adjunct and visiting professors. “Members of the public” include website visitors, consumers, and event attendees. “Locale-based individuals” include those from the EU, UK, California, foreign students, and foreign faculty.

For the second question on what types of activities present at universities or that universities engage in would trigger privacy laws / standards, the responses were analyzed and grouped where appropriate. There were thirty-two options once grouped. The options ranged from specific laws, e.g., CCPA (California Consumer Privacy Act), CMIA (California Medical Information Act—or other similar state law) and GDPR to functions of laws, e.g., biometric laws / requirements and finance laws / requirements. One response was notable in its comparison to the public square concept: “In some ways the university is the quenticential [sic] public square and privacy is not expected but there are certain data that the university gets that has or should have privacy requirements.” If one considers that Universities are typically open and that anyone can visit the grounds, the public square concept is rather apropos.

The third question on the privacy laws / requirements that are important for universities to follow were analyzed and grouped where appropriate to provide Experts with twenty-seven options in Round 2. Examples ranged from the expected FERPA to laws that address behaviors, such as data breach notification laws. Please see Appendix G for the full list. Several responses

were the equivalent to, if not verbatim, “All of them,” including these two: “Is there an option to not follow the law? So, all…” and “It’s a little flip to say ‘all of them,’ but all of them. The fact that you're a university does not mean that you don't have to be cognizant of the rules.”

The fourth question asked the Experts to identify the institutional and / or programmatic elements (in no particular order) that should be present if they were to review universities for privacy compliance. These results were from Round 1 were analyzed and grouped where appropriate to provide Experts with thirty-six options in the subsequent rounds. Examples include automated decision-making insight and processes, culture, following a framework / defining model, and third-party management (vendors and partners).

The last question in the Round 1 open-ended questions asked what risk factors are present at universities for noncompliance in terms of privacy compliance. For this question, it became apparent that some interpreted it as the risks faced (consequences) not risk factors present. Of the twenty-six responses, half of them addressed risks to Universities (consequences) as opposed to risk factors in Universities. This was clarified in subsequent rounds, but the responses listing consequences are also presented as part of the discussion in this paper. Some of the comments, like “all of them,” were not responsive to the question for purposes of itemizing options for later upvoting. Some notable responses reflected the state of privacy laws as discussed above, such as “Not sure substantially different than other institutions.” Another entry revealed:

> Risk factors include the existence not sensitive and confidential information in abundance and breadth; The likelihood or number of individuals with technical skills and likely limited professional maturity not to do something stupid. Universities hold info created about individuals during very formative years of an individual's life. Research on the

cutting edge happens here, the confidentiality of which during creation can make or break future careers.

Of those responses that related to consequences rather than risk factors, the combined responses included: regulatory (fines, oversight), loss of trust, reputational, harm to individuals (students, research participants, employees / faculty), business loss, lower enrollment. government funding loss, litigation. Responses included: “Legal, regulatory, ethical, reputational and operational” and “too many others to name.” It is possible the first response above of “Not sure substantially different than other institutions” applies to consequences as opposed to risk factors. There was no opportunity to ask the Expert to clarify. Please see Appendix G for responses to this question and the consequence answers are indicated in gray shading. Either way, it indicates that the privacy compliance environment on University campuses is akin to that of private companies, whether in regard to risk factors inhibiting compliance or consequences faced.

In order to summarize the responses in these substantive questions, nonspecific responses, e.g., “all of them,” were inherently unable to be classified into options. However, they do emphasize the comprehensive nature of data subjects and activities that trigger privacy laws, along with the number of laws that could possibly be triggered to which Universities should thereby comply. In the end, thirty-five were categorized and represented in Round 2 for upvoting.

3.6 Round 2

The survey was open from March 8–16, 2021. Twenty-five respondents started the assessment, one did not complete the assessment. This resulted in a total of twenty-four respondents, meeting the desired number of at least twenty Experts. The demographic responses were provided in

subsection 3.4 above. The open-ended questions from Round 1 were assessed and grouped into singular responses based on the subject matter expertise of the researcher. However, for the integrity of the process, overly general responses were included where possible but otherwise eliminated.

Experts were presented with four questions and asked to "vote" on the top seven responses in each question. Each question along with the responses are below, with the responses presented in ranked order as per the Expert voting. See Appendix H for Round 2 voting options and results. The types of data subjects were not included for subsequent upvoting due to the ubiquitous nature of the data subjects. This will be addressed in more detail further below.

The Experts were asked to select seven activities that Universities engage in that trigger privacy laws out of the thirty-two resulting options from Round 1. The top ten responses are presented in Table 8. The options in the table below have been reduced to the broad categories, but the options presented to the Experts for voting included the parenthetical range of options.

Table 8: Round 2: Top 10 Activities that Trigger Privacy Laws

Options in ranked order	**Votes out of 24 possible votes**
Health-related activities	21
Data operations	15
Finance	14
Vendor management	14
Student administration	13
Human capital management / employment	13
Admissions	13
Law enforcement / policing / security & surveillance	12
Counseling	10
Activities and events	6

For example, the top-ranked option is health-related activities and that is what is presented in the table. However, the full option presented to the Experts included a parenthetical with more context "research, student health, workers comp, health centers, occupational reporting, sick leave, insurance claims, reporting." For brevity, the parentheticals are not provided herein, but they are available in Appendix H for review.

On the second topic of which privacy laws that are most important for universities to follow or most relevant to the study, twenty-seven options were presented for Round 2 voting from the open-ended responses provided in Round 1. Experts were asked to select their top seven choices. The top thirteen responses, those receiving six votes or more out of twenty-four allowed, are presented in Table 9 below. All responses, including those that received less than six votes, are included in Appendix H. The top seven responses were FERPA, breach notification laws, HIPAA, state privacy laws, data retention laws, GDPR, and biometric laws.

Table 9: Round 2: Top 13 Privacy Laws Applicable to Universities

Options in ranked order	**Votes out of 24 possible votes**
FERPA (Family Educational Rights and Privacy Act)	19
Breach notification or reporting laws / requirements	15
HIPAA	15
State privacy laws	13
Data retention laws / requirements	10
GDPR (EU General Data Protection Regulation)	9
Biometric laws / requirements	9
Limiting sharing / access laws / requirements	7
Health and related laws / requirements	7
Data minimization laws / requirements	6
Consumer protection laws / requirements	6
Security laws / requirements	6
Website privacy laws and notice requirements	6

Of the programmatic elements or activities, Experts were asked to select seven (7) that they felt must be present in a university privacy program. Thirty-six options were presented from Round 1 and the top eleven voted options are presented in Table 10. All responses, including those receiving less than seven votes, are included in Appendix H. These elements included a designated privacy lead, privacy policies, a data security program, third party management, and central oversight.

Table 10: Round 2: Top 11 Important Privacy Program Elements

Options in ranked order	**Votes out of 24 possible votes**
CPO / privacy lead designated	14
Privacy policies + procedures	11
Data security policy and program (proactive)	11
Third party management (vendors and partners)	9
Central oversight	9
Monitoring, audit, assessments	8
Privacy program development and implementation	8
Training (mandatory, department-specific)	7
Data classification and handling matrix	7
Data inventories	7
Dedicated staff with appropriate resources	7

The last category presented to Experts was the risk factors that put universities at risk for noncompliance with privacy laws. Experts were asked to select seven risk factors from the thirty-five that resulted from Round 1 input. The top eleven are presented in The options on consequences or risks to Universities was not considered for additional upvoting.

Table 11. All responses, including those receiving less than four votes, are presented in Appendix H. Universities face risks from such factors as inadequate funding, decentralized and

siloed data systems, and an abundance and breadth of sensitive and confidential information. The options on consequences or risks to Universities was not considered for additional upvoting.

Table 11: Round 2: Top 11 Risk Factor Universities Face

Options in ranked order	**Votes out of 24 possible votes**
Inadequate funding for data protection programs (privacy / security)	18
Decentralized and siloed data systems	15
Existence of sensitive and confidential information in abundance and breadth	13
Lack of University leadership focus & evangelization of data privacy as a priority	11
Lack of a compliance culture (e.g., faculty and staff who feel they have the autonomy to not follow established policies and procedures)	10
Extremely diverse activities, data sets, and data subjects	10
Lack of awareness of laws and policies (and the reasons behind them)	9
Outdated systems	8
Poor data protection controls	7
Lack of employed or contracted staff that understand privacy	7
The huge number of sectoral activities at play in the average university	7

Much like types of data subjects, the consequences are rather well-known and ubiquitous. Once Round 2 was complete, the votes were tallied and then reduced to the top ten or where the natural vote count broke at or above number ten. These lists were then presented in Round 3 for the last portion of the Delphi method.

3.7 Round 3

The survey was open from March 18–30, 2021. Thirty-three Experts started the assessment, five did not complete the assessment. This resulted in a total of twenty-eight Expert responses, meeting the desired number of at least twenty Experts. Demographics were provided in subsection 3.4 above. The upvoted responses from Round 2 were assessed and presented to the

Experts for the last round. However, an additional optional open-ended question was added at the end, please see question 5 below.

Experts were presented with the four questions as listed in Round 2 and asked to vote on the top three (3) responses in each question out of the top responses in each question. The number of top responses varied based on the natural breaking point of the respective responses resulting in the top 10, 13, 11, and 11 respectively. Each question along with the upvoted responses are below, with the responses presented in ranked order as per the Expert voting. There were thirty Experts active in this Round, so the voting results are out of thirty possible votes. The responses to these four questions along with the additional optional open-ended question are presented below.

The first question was to select three out of the ten top voted activities present at Universities or that Universities engage in that would trigger privacy laws or standards. Like Round 2 above, the parenthetical, if there was one, has been eliminated from Table 12 below. The parentheticals were available to the Experts during the round, as can be seen in Appendix I. The top category upvoted was health-related activities. These activities included research, student health, workers comp, health centers, occupational reporting, sick leave, insurance claims, and reporting—and comprised the parenthetical presented for Expert consideration.

Table 12: Final Rank: Activities (top four)

Options in ranked order	**Votes out of 30 possible votes**
Health-related activities	24
Student administration	21
Human capital management / employment	9
Vendor management	8

Student administration was the next largest category and included academics, analytics, grading, class lists, surveys, attendance, registration, and discipline. Human capital management and vendor management round out the top four voted activities.

On the third question for the privacy laws that are most important for Universities to follow or most relevant to this study, the Experts were presented with thirteen options. They were asked to select three. The votes shown in Table 13 are out of a possible thirty votes. All thirteen options with their corresponding votes are presented below. The top law was FERPA, which given the applicability to Universities, is not surprising. The next five are general types of laws and not specific laws. These include data sharing or access laws, state privacy laws, health and related laws, breach notification laws, and security laws. More about each of these is covered in Chapter 5, Doctrinal Legal Research.

Table 13: Final Rank: Privacy Laws (all thirteen)

Options in ranked order	**Votes out of 30 possible votes**
FERPA (Family Educational Rights and Privacy Act)	18
Limiting sharing / access laws / requirements	11
State privacy laws	9
Health and related laws / requirements	9
Breach notification or reporting laws / requirements	8
Security laws / requirements	7
GDPR (EU General Data Protection Regulation)	6
HIPAA (Health Insurance Portability and Accountability Act)	4
Data retention laws / requirements	4
Website privacy laws and notice requirements	4
Data minimization laws / requirements	4
Biometric laws / requirements	2
Consumer protection laws / requirements	1

The next set of upvoting questions is the privacy program elements. Experts were asked to select their top three out of eleven options. This question had less voting range than the others with the top option having sixteen votes and the last option having three votes. The top three programmatic elements were privacy program development and implementation, a designated privacy lead, and third-party management, including both vendors and partners. See **Table 14**.

Table 14: Final Rank: Privacy Program Elements (top 3)

Options in ranked order	**Votes out of 30 possible votes**
Privacy program development and implementation	16
CPO / privacy lead designated	14
Third party management (vendors and partners)	11

The last question of the upvoting was for the Experts to vote on three of the top eleven risk factors for noncompliance with privacy laws at Universities. The top risk the Experts feel Universities face is decentralized and solid data systems with the next biggest risk being inadequate funding for data protection programs, both privacy and security. See Table 15. The next three tied at eleven votes each. They are a lack of University leadership focus and

Table 15: Final Rank: Risk Factors (top five)

Options in ranked order	**Votes out of 30 possible votes**
Decentralized and siloed data systems	16
Inadequate funding for data protection programs (privacy / security)	13
Lack of University leadership focus & evangelization of data privacy as a priority	11
Existence of sensitive and confidential information in abundance and breadth	11
Lack of a compliance culture (e.g., faculty and staff who feel they have the autonomy to not follow established policies and procedures)	11

evangelization of data privacy as a priority, the existence of sensitive and confidential information in abundance and breadth, and a lack of a compliance culture (e.g. faculty and staff who feel they have the autonomy to not follow established policies and procedures).

The extra question added to Round 3 asked whether the experts would like to add any comments about managing privacy at us universities. Three Experts submitted comments. They are provided below verbatim. One opined how difficult it was to select three because privacy is so very complex, another explained not selecting FERPA, and the last comment reiterated the risk factors. The first comment is:

> it was really difficult to select on three in each category because the complexity of privacy laws applied to the wide range of activities at universities is enormous. My recommendation would be to have centralized management of privacy-focus areas, e.g., hospitals, research, student records, personnel—and treat them like departments reporting up to a chancellor. There needs to be one person who has visibility across the whole system and it cannot be the CISO. Privacy laws need someone who understand that security is one part of data governance.

The next response was that "Universities of course must follow FERPA, so i [sic] did not select it. Privacy programs, otherwise, are the same as any other company. Perhaps worse because universities aren't managed like a company, with clear responsibilities, central oversight, and corporate social responsibility goals." The last response reinforced the risk factors with "[t]he problem with privacy at universities is there is so much data in outdated systems, lost repositories, privacy programs in siloes who grew organically with no centralization and now, there are a whole lot of drill sergeants but no general." These comments from the Experts

continue to emphasize that privacy compliance at Universities is not a simple undertaking and that there is a confluence of factors that add to the complexity of compliance efforts.

3.8 Chapter 3 Summary

The Delphi method undertaking was valuable to have experts identify triggers and complexity of privacy compliance at Universities. The results of the Delphi will be used to drive the following two chapters, Document Analysis and Doctrinal Legal Research. This added a level of academic rigor and objectivity to the undertaking rather than relying on the researcher's own professional expertise. The findings reiterated that this line of inquiry is relevant and necessary in the field of privacy, especially as it relates to Universities. However, it also reinforces the complexity of fully understanding the factors that contribute to or offset the privacy compliance efforts in a CAS with a CAS, given the layers of both the setting within Universities and accounting for privacy law.

CHAPTER 4

DOCUMENT ANALYSIS

This element of the overall study was dictated by the results of the Delphi method to drive the search to determine if the elements are present. Each of the sample Universities were reviewed for the consensus elements identified by the Experts in the Delphi portion. Using available resources, such as the universities' website, media, and annual reports, it was determined whether the elements identified by the Delphi were present. According to the Experts, if certain elements (data subjects, activities) are present, privacy laws are or may be triggered. The Experts also informed us what privacy laws are most important or critical at Universities, what risk factors are most common that would cause a privacy program to fail, and what programmatic elements should be present in a successful privacy program.

This Document Analysis portion (construed broadly to include publicly available information found online regardless of the format, e.g., pdf available online or webpage) was conducted on a purposive sample of Universities as described in more detail below. Document analysis is an accepted qualitative process, often used in concert with other methods, and yields data through content analysis (Cohen 1999). Each of the University websites was reviewed to identify key words using the site's search functionality. Where warranted, further assessment was performed to ensure the search returned valid results for the purposes of this study. This chapter presents the methodology first, followed by the findings, and concludes with a short summary.

4.1 Document Analysis Methodology and Sample Selection

The first step was to identify a sample. The top two schools were selected from both private non-profit universities and public universities that rank as the number 1 and 2 of their classifications based on an industry-accepted ranking, the U.S. News and World Report rankings. The rationale was that the top-ranked Universities may be more mature in their processes and that there may be a notable difference between the identified Universities and the randomly selected ones. Two Universities in each classification were randomly selected to round out four institutions in each classification. This mix was designed to include institutions that are highly regarded and likely have a wide range of programs and activities, but also consider a random sampling within each category.

The U.S. News and World Report's Best Colleges Rankings for 2021 was consulted to identify the top two ranked public and private non-profit universities (2021). The top two public schools were both within University of California system. The first was Los Angeles and the second was Berkeley. Given that both are University of California campuses, and the resulting analysis may lack diversity, the third-ranked public college was also included, the University of Michigan at Ann Arbor. The top two national universities were Princeton University and Harvard University, respectively; both are privately-owned institutions. The list was not specifically sorted by privately owned as that was not a free option for the research access, but the two schools were also cross-referenced with the list generated from the database discussed below. Both were included in the list of private, non-profit universities.

According to the National Center for Education Statistics of the Institute of Education Sciences, the "statistics, research, and evaluation arm of the U.S. Department of Education"

(2021) there are 807 public institutions of postsecondary education which grant four-year degrees in the United States and 1,685 private non-profit universities. Private for-profit universities were eliminated from the considerations given the differences in the business operating model. The database was queried for two factors; level of institution: granting four-year degrees and control of institution: public and private non-profit. The resulting list was exported in a .csv format, including the search criteria. The list of universities was then sorted by public or private and separated into two tabs and saved in a Microsoft Excel spreadsheet.

The random sampling was then conducted using the online random number generator at www.random.org. The number range for each category was defined (1–807 for public universities and 1–1685 for private nonprofit universities) and the tool selected a random number. There was not an option to select two numbers, so the selection process was repeated for each category, with plans in place to repeat the process if the number was repeated or if the numbers one or two were generated. In addition, if the selected institution was a branch campus or division of a main institution, the main institution would be the selection, not the branch or campus unless the university functions in such a way that the locations are essentially their own entities, such as with the top two public universities both being University of California. The generated numbers were 339 and 488 for public universities and 767 and 992 for private nonprofit universities.

After matching the numbers to the automated line numbers in the spreadsheet, the resulting list was nine institutions, five in the public category and four in the private non-profit category. See Table 16 for the specific list.

Table 16: University Sample Population

Public Universities	Private Non-profit Universities
1,2: University of California (Los Angeles, Berkeley)	1: Princeton University
3: University of Michigan	2: Harvard University
339: Ohio State University	767: Lincoln Christian University
488: Stone Child College	992: Northwest University

Once identified, the institutions' websites were reviewed for publicly available information to assess for the five items identified in the Delphi method: categories of individuals that trigger privacy / data protection requirements, activities that trigger privacy requirements, privacy laws applicable to Universities, necessary privacy program elements, and risk factors that may prevent Universities from complying with privacy laws. All but the first was voted on by Experts in Rounds 2 and 3.

Both content review of the website and analysis of pertinent documents residing on the websites was performed. Further, internet searches for the name of the university in combination with the item was conducted if the website search was inconclusive. This was particularly useful for the programmatic elements and risk factors.

4.2 Categories of Data Subjects and Activities

The first two categories, data subjects and activities, if present at Universities will identify if the university provides services or products to certain types of data subjects or engages in certain activities. The items in each of these categories were identified by the Experts as the most relevant items that trigger privacy laws. According to the Experts, if these items are identified, then the element triggers one or more privacy laws that may apply and would then suggest the University is subject to privacy laws. This aspect of the research demonstrates that

there are more elements to consider than merely accepting funding from the federal government which triggers FERPA, as mentioned above in Chapter 2.

Certain privacy laws are triggered merely by the data subjects that may be present. For example, the GDPR is triggered if an entity offers goods or services directly to individuals in the EU. Universities might trigger the GDPR by deliberately reaching out to students in the EU to offer exchange programs; to market online education programs or conduct research on individuals in the EU; or to recruit professors or speakers from the EU. There is no number of individuals that needs to be involved in order for the University to be subject to the GDPR. Certainly, a practical consideration would be that a university who only recruits one person as a speaker would certainly not draw the level of compliance needs that operating a satellite office in the EU would require.

Likewise, having online services that appeal to children under the age of 13 would implicate COPPA. Also, having patients or research subjects could certainly trigger the Common Rule or even HIPAA. As explained in Chapter 2, it is not enough to merely have patients, one must be engaged in certain activities to trigger HIPAA. Conversely, just having employees would trigger GINA or having employees with disabilities would trigger the ADA.

As mentioned above, the types of data subjects that would trigger privacy laws were not included in Rounds 2 or 3 due to the innate presence of most objects at Universities. Data subjects are closely related to activities. For example, like COPPA mentioned above. It is not just the "presence" of children that matters, it is whether or not the website is directed at children. Therefore, it is not enough to identify the type of data subject, but the activity associated with the data subjects must also be assessed. Privacy laws may be triggered off one or both. This is the

same consideration for HIPAA. It is not just the presence of patients; it is the contemporaneous activity that goes along with them.

Of the fifteen types of data subjects identified in Round 1, all Universities presumably have nine of them: students, staff, families, visitors, vendors, alumni, faculty, members of the public, and payors of student fees. Six categories remain: patients, research subjects, customers, donors, locale-based individuals (e.g., from EU, UK, CA), and people with disabilities. Only these six types of data subjects were included in the Document Analysis.

Findings

First, the Universities were assessed for the types of data subjects, as presented below in Table 17. All sample Universities address donors, people with disabilities, and customers in their available documentation. Most of the Universities, 78%, engaged in research with processing data on research subjects. As discussed in Chapter 2, such activities would require an evaluation of research laws for compliance requirements, such as the Common Rule. Two-thirds of the sample process data on patients, triggering healthcare laws potentially on local, national, and international levels especially if combined with locale-based data subjects. Two-thirds of the sample process data on individuals within certain locales, such as California or the UK, which have laws that are triggered in relation to the location of individuals.

Table 17: Types of Data Subjects in Universities

Identified Presence	**patients**	**research subjects**	**customers**	**donors**	**locale-based**	**people w/ disabilities**
% Yes	67	78	100	100	67	100
% Not identified	33	22			33	

The Universities were next assessed for the activities that might trigger privacy laws as identified by the Experts. The top three results were health-related activities, student administration and human capital management. Health-related activities includes research, student health, workers comp, health centers, occupational reporting, sick leave, insurance claims, and reporting. Likewise, student administration was further detailed as academics, analytics, grading, class lists, surveys, attendance, registration, and discipline. Human capital management / employment included both staff / faculty/contractors, applications, management, benefits, salary, contracts / contractors, performance reviews, student reviews, and publications. All Universities in the sample have activities related to health-related activities, student administration, and human capital management (HR). As broad categories, this is not surprising. The difference is in the details of the activities found.

As shown in Table 18, not all sample schools engage in all the activities. "Not identified" indicates that no information was found, not that it does not exist. Further, the information on student health, for example, varies across the sample. At one University, a tribal college offering one bachelor's degree, the only reference to student health was on COVID-19 data. Meanwhile, the top-ranked schools, such as the University of California and Princeton, have full-service student health centers active on multiple campuses.

Table 18: Health-related Activities in Universities

	health research	**student health**	**occup. reporting**	**sick leave**	**insurance claims**	**health metrics**
Identified Presence						
% Yes	89	100	67	78	67	100
% Not identified	11		33	22	33	

This same consideration applies to the other activities: student administration and human capital management. The overarching activity is present, the nuances in the details may or may not be derived from the information available online. Please see Table 19 for detailed activities within student administration. However, privacy laws are rarely triggered by nuanced activities in student administration. It is enough that personal data on students is processed. Yet, as discussed above, it is not the processing of student information that triggers FERPA, it is whether the Universities accept funding from the U.S. Department of Education. As seen in the upcoming findings, all schools in the sample indicated they are subject to FERPA.

Table 19: Student Administration Activities in Universities

	academics	**analytics**	**grading**	**class lists**	**surveys**	**attendance**	**registration**	**discipline**
Identified Presence								
% Yes	100	89	100	67	89	100	100	100
% Not identified		11		33	11			

Human capital management is similar, although, there is no specific privacy law that applies to this broad category of activities, like FERPA to students. Privacy for employees is grounded in constitutional law, such as was discussed in Chapter 2 and case law. Human resources privacy, in large part, relies on a combination of laws and whether individuals have a reasonable expectation of privacy. Given this understanding, the sample schools were not searched for listed items in human capital management. The implications of privacy for employees and activities related to them will be discussed further in Chapter 5.

4.3 Applicable Privacy Laws

The third category comprises the most common or the most important privacy laws that apply to Universities as identified by the Experts. The top four items ranked by Experts are presented in Table 20 below. Four options were chosen, because FERPA is a natural option given the educational setting and there was a tie for third place. This also contributes to the Doctrinal Legal Research section. In the assessment of websites and documents, the search functionality within each University's website was searched for the term specified. For some of the privacy laws or types of laws, this comprised multiple terms and respective searches, reflected later in Chapter 5.

Table 20: Privacy Laws Identified in Universities

	FERPA	**sharing / access**	**state laws**	**health laws**	**breach notices**
Identified Presence					
% Yes	100	78	45	78	67
% Not identified		22	55	22	33

This table shows what was identified through analysis of the information available. For example, every state in the United States has passed breach notification laws (please see Appendix B for a full list); yet three of the sample schools did not have information on breach reporting, including how students could report a data breach. Given that California is the only state with an active state privacy law, the only Universities subject to the law would be those that meet the triggering requirements of doing business in California and having a certain amount of data or revenue, as provided for in the CCPA, section 1748.100.

4.4 Program Elements and Risk Factors

The last two categories are programmatic elements that should be present in a university privacy program and risk factors that put Universities at risk for noncompliance. Given the broad scope of these two categories, the website and document reviews are more contextual. For this section, the University search function as listed above was used, along with review of the respective privacy policies, annual reports, and general online searches with the name of the school and the identified terms. The goal was to identify if the identified elements were present, not to evaluate the quality or extent of the elements.

The top three program elements that the Experts determined needed to be present in a University privacy program were privacy program development and implementation, a Chief Privacy Officer or designated privacy lead, and third-party management (vendors and partners). As seen in Table 21, it was possible to determine if the three factors were present in some fashion or not present. The challenging part of this was to ascertain the depth or the extent of the development. For example, Northwest University had no information available on its vendor management program. However it was easy to identify that they have genders and that they intend to manage them, because this was listed in several of the job descriptions that were available. The available role included job duties that specified supervising one or more identified vendors. In contrast, some of the other Universities had their policies for vendor management available for consideration.

Table 21: Programmatic Elements Identified in Universities

Identified Presence	Privacy Program development	CPO / privacy lead	Vendor Management
% Yes	67	67	89
% Not identified	33	33	11

In particular, the maturity of programs was difficult to assess, especially if one of the only factors to measure of the presence of a designated privacy lead. In 2019, Educause had thirty members on its Chief Privacy Officer roster (Johnson 2019). A review of the International Association of Privacy Professionals (IAPP) member registry found six professionals with privacy in their titles at Universities, but also three in-house attorneys at Universities, two in executive offices at Universities, and several others in IT, information security, and some level of compliance. This is not a confirmed count, but it does suggest that the field is immature and available for growth. Of the sample, 33% of the Universities sampled had chief privacy officers, 33% had privacy vested in the chief information officer, and 33% had no privacy officer, other than someone to oversee FERPA inquiries, typically the registrar's office.

The Experts identified the factors that put Universities at risk for noncompliance with privacy laws. These risk factors can also be considered the critical challenges that Universities face in privacy compliance efforts. They are (a) decentralized and siloed data systems; (b) inadequate funding for data protection programs (privacy / security); (c) lack of university leadership focus and evangelization of data privacy as a priority; (d) existence of sensitive and confidential information in abundance and breadth; and (e) lack of a compliance culture. The last factor of lacking a compliance culture incorporates faculty and staff who feel they have the autonomy to not follow established policies and procedures. There are five listed because there was a three-way tie for third place.

This last section was the most difficult to assess via public information. This section was heavily reliant on a variety of documentation aside from merely the University websites. Although unable to substantiate with metrics and in-depth study, all sample Universities appear

to have all of these risk factors to some degree. The level of degree cannot be determined without more targeted research. No sample University appeared to have an abundance of executive leadership evangelization of privacy, although the University of California has quite an amount of information publicly available on a recent data breach impacting student information (See University of California, Accellion breach, 2021).

In general, Universities need to take these factors into account when developing their privacy programs. If they do have multiple campuses, like the University of California, will they have centralized privacy oversight with campus officers? If there are no privacy laws for them to comply with except FERPA, will they have their registrar manage privacy, such as it is? These are aspects of a privacy program that Universities must consider. Budget is also important. In 2020, dwindling income decimated privacy programs, especially given that privacy is still developing at many Universities (Educause 2020). Although, COVID-19 did also raise awareness of privacy issues. 62% of respondents to an Educause study report that the privacy program reports up through a privacy office, where 39% reported that privacy reports to the information security office (Burns 2020). However, Educause provides that:

> At many institutions, the title and duties of a privacy officer have regularly been attached to the already existing positions of CISOs. Unfortunately, our interviewees who held both the CISO position and the privacy officer title or privacy management duties reported that the information security side of their job is so demanding that they can only dedicate a small portion of their time—on average 10%—to their privacy duties. (Burns 2020)

As for HIPAA, about half respondents state they manage HIPAA, where the other half reports there is a separate HIPAA office (Burns 2020).

Without deeper research into the risk factors, it is impossible to discern if the Universities are experiencing such risks. Although some of the Universities do make their budgets public, there is no mechanism to determine if privacy is underfunded, other than the information available through other resources. It was likewise impossible to determine if the data systems are decentralized or siloed—which is different than privacy offices being decentralized. The physical location of systems does not equate to the responsibility distribution among professionals or offices. One of the risk factors was notable by its absence of evidence. None of the Universities were noted to have leadership that evangelizes privacy. And another risk factor—the breadth and abundance of sensitive and confidential information—was established through earlier elements.

4.5 Chapter 4 Summary

This analysis in general suggests that the Universities have addressed the needs associated with or stemming from the traditional view of privacy at Universities. Even those without designated privacy officers have an individual or office designated to manage FERPA. Yet, overwhelmingly, the Universities engaged in data processing, both for types of data subjects and activities, that the Experts determined would trigger privacy laws. The Document Analysis illustrated that Universities are largely aware of applicable privacy laws. Information on privacy programs was feast or famine. Unless there was extensive information on their privacy offices or practices, there was essentially no information to review. The risk factors are, in large part, unable to be evaluated other than two risk factors; Universities have an abundance and breadth of confidential and sensitive personal data and there appears to be a notable lack of executive evangelism of privacy.

CHAPTER 5

DOCTRINAL LEGAL RESEARCH

Analyzing how Universities manage privacy compliance necessitates understanding why managing privacy is a topic to consider at Universities and fundamentally, is there a reason why privacy needs to be managed one way versus another. In a study of this nature, the law is critical, yet in presenting this information, the Doctrinal Legal Research methodology is intended to present it in a fashion acceptable to the non-legal scholar environment (Hutchinson and Duncan 2012).

One of the most bemoaned characteristics of legal research is that legal researchers typically avoid explaining the methodology behind the research (Fourie 2015; Kharel 2018; Hutchinson and Duncan 2012). To avoid this flaw, the intent is to ground the legal research by basing it on the results of the Delphi method and to explain the methodology. Using the outcomes of the Delphi, the Doctrinal Legal Research will use the top-voted laws or areas of law to drive research on how the law applies to Universities, the compliance requirements, and the potential and form of enforcement. Further, the findings from the Document Analysis as described above will be used to determine the extent to which the laws apply to the sampling of Universities examined. Lastly, the key elements of Complexity Theory: self-organization, coevolution, and nonlinear dynamics are applied to the outcomes. Thus, Doctrinal Legal Research is a fundamental aspect of this engagement, one that intends to "provide explicit normative comment (how things should be) in order to formulate needed proposals for improvement" (Fourie 2015, 96; internal cites omitted).

Given the literature review and fundamental concepts provided in detail in Chapter 2, this section will not explain privacy law itself, but rather contextualize the research to better understand the state of privacy compliance at Universities, building on the information provided *supra*. Below is an overview of the applicable results of the Delphi method followed by the respective legal assessment and understanding of the results.

5.1 Reminder of Applicable Delphi Results

The results of the second question of Round 3 asked Experts to select their top three privacy laws that Universities need to follow or that were most important for this study. Please see Table 22. In the prior chapter, only the top five were assessed in the Document Analysis. In this chapter on Doctrinal Legal Research, all thirteen are addressed.

Table 22: Results of Privacy Laws

Ranked Order	**Total # of Votes**
FERPA (Family Educational Rights and Privacy Act)	18
limiting sharing / access laws / requirements	11
state privacy laws	9
health and related laws / requirements	9
breach notification or reporting laws / requirements	8
security laws / requirements	7
GDPR (EU General Data Protection Regulation)	6
HIPAA (Health Insurance Portability and Accountability Act)	4
data retention laws / requirements	4
website privacy laws and notice requirements	4
data minimization laws / requirements	4
biometric laws / requirements	2
consumer protection laws / requirements	1

Although, as explained in Chapter 2, FERPA is not applicable by default to all universities, it is certainly applicable to the vast majority. Given that the intent of the Delphi was to let the Experts determine the issues, it is possible that an in-person session may have elicited opinions on whether to include FERPA in the upvoting sections or simply include it by default. A comment was also submitted on this point in the additional open-ended question in Round 3:

> Universities of course must follow FERPA, so i [sic] did not select it. Privacy programs, otherwise, are the same as any other company. Perhaps worse because universities aren't managed like a company, with clear responsibilities, central oversight, and corporate social responsibility goals.

Regardless, FERPA was ranked by the Experts as the top privacy law that is most important or relevant for Universities to follow. The Document Analysis demonstrated that premise to be true as 100% of the sample Universities addressed FERPA. However, there was a difference in how FERPA was addressed, ranging from one mention in the student handbook with contact information for the registrar to elaborate web pages with quite a bit of information on FERPA.

Despite being conducted fully remote with no interaction amongst Experts, the Delphi method was effective. In the first round, the open-ended questions on which laws are most important had answers that ranged from “all of them” to specific laws listed. As the upvoting began in the subsequent rounds, the most important or relevant laws that received the most votes were by function rather than specific laws. In the top thirteen laws, only three are specific laws: FERPA, GDPR, and HIPAA. The remainder are general groupings of laws, e.g. state privacy laws, data retention laws / requirements, and security laws / requirements. This is how they will be grouped and addressed below.

5.2 Specific Laws

FERPA

As mentioned above, it is not surprising given the sectoral nature of privacy law in the United States, and that FERPA is the education privacy law. Congress has amended FERPA eleven times since it was enacted in 1974, in many cases to broaden disclosure requirements or to modify the definition of an educational record. FERPA includes an acknowledgement of the privacy rights of students under the Individuals with Disabilities Education Act (34 CFR 300.610–300.626) which indicates a coordination of privacy that is notably lacking with other U.S. privacy laws, such as HIPAA. HIPAA provides an exemption for FERPA educational records and treatment records (45 CFR 160.103), but the exception falls short of coordination. Some of the criticism FERPA has faced have centered on its deficiencies on vendor management, private right of action, and enforcement (U.S. House of Representatives 2015).

FERPA includes a provision wherein medical and psychological treatment records of students at postsecondary institutions are excluded from being considered "education records" and are considered "treatment records" (34 CFR § 99.3). Treatment records must be made, maintained, and used only in connection with treatment and disclosed only to those individuals providing the treatment. These records may be disclosed outside these parameters if the student consents or if the disclosure meets one of the exceptions in FERPA (34 CFR § 99.31(a)). However, once it is shared outside a treatment context, it no longer warrants protection as a treatment record and is then considered merely an educational record, which is protected but to a different extent.

In the Document Analysis portion, each of the Universities were found to be subject to FERPA. In general, their FERPA officers sat in the registrar offices with support from legal, HIPAA officers sat in the medical centers if there were any, and other privacy functions were spread amongst IT, information security, and compliance. Universities that violate FERPA are subject to inquiry and potential cessation of government funds (U.S. Department of Education, Office of Inspector General 2018).

As an example, The University of California, Irvine, received a letter from the U.S. Department of Education dated July 28, 2019, addressing a complaint received on July 22, 2016 (Miller 2019). The university had denied a student's FERPA request in part due to 126 pages being considered attorney-client privilege. The letter reinforces that FERPA does not explicitly exempt documents under attorney-client privilege; the U.S. Department of Education recognizes that a school may deny a request for such reasons. The complaint was dismissed, and the university cleared of any wrongdoing. It took three years from the time the complaint was initiated to reach its resolution.

In 2018, the Office of the Inspector General (OIG) within the United States Department of Education issued a letter with audit findings regarding how the office manages the investigations of complaints (U.S. Department of Education, Office of Management 2018). The OIG found that the department was significantly behind on processing complaints, estimated at greater than two years, and reported that "[m]ultiple factors contribute to the backlog, including a lack of resources to timely investigate all complaints and unresolved FERPA policy issues that impede complaint investigations" (2018, 12). The letter also included information about privacy laws that this office managed:

> . . . two other laws related to student privacy: the Protection of Pupil Rights Amendment and the military recruiter provisions of the Every Student Succeeds Act. However, Privacy Office officials told us that 95 percent or more of the Privacy Office's student privacy workload is related to FERPA. In addition to its work on student privacy, the Privacy Office administers other statutes for the Department, such as the Freedom of Information Act, the Privacy Act, the Federal Records Act, and the Paperwork Reduction Act (Office of the Inspector General 2018, 9).

Thus, although no further violations were identified for the sample population, that does not mean that there are not complaints in process at this time that have not been finalized. On the Practical side, FERPA has not had a reputation for active enforcement activities, unlike the Office for Civil Rights discussed below.

HIPAA

Given the student medical clinics commonly found on University campuses, people quite often hold the misconception that these medical records are subject to HIPAA (Teeter 2017). More information is provided in the section below addressing HIPAA as to what types of institutions and records are subject to HIPAA. Unfortunately, this seeming overlap creates quite a bit of confusion. One such example involves rape victims on campus seeking medical treatment from the on-campus clinics only to discover later that their records were provided to the University legal offices in preparation of legal defenses (Foden-Vencil 2015). Students were often surprised to find that their records were shared in such a way, but the purpose—for the legal defense of the university—is an exception permitted under FERPA disclosures although it would not be under

HIPAA. This is one of many reasons there is tension between FERPA and HIPAA enforcement and confusion in the relevant population.

HIPAA applies to campus health clinics if they qualify as covered entities under HIPAA by providing health care to those who are not students and engaging in certain electronic transactions. Of the sample Universities, 67% had health clinics for students, 78% addressed healthcare laws, such as HIPAA, in their information and materials. The University of California, Office of the President has posted that their Board of Regents designated the University of California as a HIPAA hybrid covered entity in May 2002 (2021). Further, the UC as a whole is "a Single Health Care Component for the purposes of complying with the HIPAA Rule . . . medical centers, medical clinics, health care providers, health plans, student health centers." They did exclude the research function. "Accordingly, research health information that is not associated with a health care service is not subject to the HIPAA Privacy and Security Rules." They do include that "[o]ther state and federal laws govern privacy and confidentiality of personal health information obtained in research."

Universities may also be subject to HIPAA in their role as employers with self-insured health plans or via health research initiatives, or if health care was provided to students by non-University professionals who independently billed for their services. In the latter case, the records would not then belong to the Universities and would not qualify as treatment or educational records under FERPA. Campus health clinics could also potentially be subject to HIPAA if they qualified as business associates, but such has not been a common situation.

Although the U.S. Departments of Education and Health and Human Services issued a joint statement in 2008 to clarify how the two laws interact with each other, the confusion

remains. Privacy laws are not well understood in isolation, and interactions among them add exponential layers of complexity. In this way, the omnibus privacy laws found in other regions, such as the GDPR, are simpler to determine if they apply to certain data or entities given their general applicability to personal data and to entities that handle such personal data. There may be exceptions for government actors, but not nearly to the extent of the exemptions or subject matter overlap found in U.S. laws.

Without doing a deeper analysis as to how HIPAA applies, such as being a self-insured employer, offering medical services to non-students and billing for insurance, or functioning as a business associate, it is difficult to ascertain the specifics of the application. However, under HIPAA, covered entities are required to have privacy officers. Covered entities and business associates both are required to appoint security officers. There are also certain controls that must be in place, such as physical, administrative, and technical safeguards.

The Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS) enforces HIPAA and requires both covered entities and business associates to report any data breaches over 500 people or records impacted (HIPAA, 45 C.F.R. §§ 164.408(c)). These reports are publicly available with basic metrics on the HHS website (U.S. Department of Health and Human Services 2021) According to their records, there are currently 30 cases under investigation where the entity has either “university” or “college” in their names. See Table 23. These current cases had a total of 859,468 records breached. Of those cases that are closed, there were 163 breaches impacting over 7 million records, 7,156,980 to be exact.

Table 23: HIPAA Breaches at Universities / Colleges

	# entities Under Investigation	# records	# reports closed	# records
University	29	832,393	147	7,105,885
College	3	27,075	16	51,095
TOTALS	32	859,468	163	7,156,980

Of those closed, the organization was a business associate in four cases, a health plan in seven, and the remainder (152), the university or college was a health care provider. In only seventeen cases was the breach caused by a business associate of the university or college. For those currently under investigation, of which two date back to a reported date of 2019, there were three reports where the college or university was a business associate, one as a health plan, and the remaining twenty-eight, the entity was a health care provider. In nine of the open cases, there was a business associate involved, but in two of those the university or college is a business associate, so the exact situation is not known as the details are not known until the case is closed—except through the media. Looking at both open and closed cases, in the overwhelming majority of cases, the university or college was a covered entity. In the enforcement realm, nine Universities had penalties issued against them since 2008 (U.S. Department of Health and Human Services 2021). See table 24 for details. The total amount was over $16.3 million. As clearly evidenced by the reportable breaches, although campus health clinics and university activities are only subject to HIPAA under certain circumstances, there is a significant amount of HIPAA activity associated with Universities. In our sample population, 67% had associated medical clinics or hospitals. Each of them had HIPAA officers, who were not the chief privacy

Table 24: HIPAA Enforcement Against Universities

Date	Entity	Amount	Issue /Link
July 6, 2011	University of California, Los Angeles	$865,500	Resolution Agreement with the University of California at Los Angeles Health System
May 21, 2013	Idaho State University	$400,000	Idaho State University Settles HIPAA Security Case for $400,000
May 7, 2014	Columbia University	$1,500,000	Data Breach Results in $4.8 Million HIPAA Settlements
December 14, 2015	University of Washington Medicine	$750,000	$750,000 HIPAA Settlement Underscores the Need for Organization Wide Risk Analysis
July 18, 2016	Oregon Health & Science University	$2,700,000	Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University
July 21, 2016	University of Mississippi Medical Center	$2,750,000	Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC)
June 18, 2018	The University of Texas MD Anderson Cancer Center	$4,348,000	Judge rules in favor of OCR and requires a Texas cancer center to pay $4.3 million in penalties for HIPAA violations
November 5, 2019	University of Rochester Medical Center	$3,000,000	Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA Settlement
November 19, 2020	University of Cincinnati Medical Center, LLC	$65,000	OCR Settles Twelfth Investigation in HIPAA Right of Access Initiative
	total	$16,378,500	

officer for the university. Therefore, unlike the rather straightforward, simple, and benign FERPA, HIPAA can be confusing, complex, and carry hefty penalties.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act, (GLBA), also known as the Financial Modernization Act of 1999, effective as of May 23, 2003, addresses the safeguarding and confidentiality of customer

information held in the possession of financial institutions such as banks and investment companies. This law was not ranked by the Experts, but it would be a disservice to Universities to not cover it, however, lightly, in this research. GLBA contains no exemption for colleges or universities. As a result, educational entities that engage in financial activities, such as processing student loans, are required to comply. GLBA and other emerging legislation could result in standards of care for information security across all areas of data management practices both electronic and physical (employee, student, customer, alumni, donor, etc.). St. John's University has posted that it "has adopted a Customer Compliance Program for certain highly critical and private financial and related information." St. John's explains that their compliance program "applies to customer financial information (covered data)" that it "receives in the course of business as required by GLBA as well as other confidential financial information included within its scope" (St. John's University, Information Technology 2021).

Educause provides the following:

> This law [the GLBA] applies to how higher education institutions collect, store, and use student financial records (e.g., records regarding tuition payments and/or financial aid) containing personally identifiable information. GLBA regulations include both a Privacy Rule (16 CFR 313) and a Safeguards Rule (16 CFR 314), both of which are enforced by the Federal Trade Commission (FTC) for higher education institutions. Colleges and universities are deemed to be in compliance with the GLBA Privacy Rule if they are in compliance with the Family Educational Rights and Privacy Act. (Educause 2021)

They continue by alerting educational institutions to an audit program by the Office of Management and Budget in collaboration with the Department of Education's office of Federal

Student Aid (FSA). In this alert, Educause advises institutions of higher education to review one provision in the audit relating to the "FSA Program Participation Agreement that speaks to the GLBA Safeguards Rule, as well as two provisions in the Student Aid Internet Gateway Agreement that address data breach issues, since these agreements state each college or university's compliance obligations" (Educause 2021).

According to the Campus Computing Project, all private Universities reported 100% compliance with the GLBA and 96.3% of public Universities reported being fully compliant (Green 2019). The GLBA is at its essence more of a security standard than a privacy one, despite its protestations otherwise, partially due to the statement above about FERPA compliance equating to GLBA compliance when it comes to privacy. Universities needed only to implement the security provisions of GLBA to effectuate compliance.

The EU's GDPR

The EU passed the GDPR in 2016 with an effective date of May 25, 2018. The GDPR replaced Directive 95/46/EC, which was not a regulation. It was a directive, indicating all member states had to meet certain criteria and results in a patchwork or national laws that was difficult for companies to do business across all of the EU without violating one or more laws by trying to meet the others (Detlev and Hickman 2019). In contrast, the GDPR set one law for all member states, thus eliminating the patchwork of laws. Member states are, of course, allowed to pass more protective laws within their national borders (GDPR, Chapter 9, e.g., for health care laws or laws protecting minors GDPR, article 8).

The GDPR also has extensive extraterritorial provisions that apply to data processing by controllers and processors. Data processing refers to any collection, use, sharing, manipulating,

storing, or deleting personal data – anything that involves personal data is processing. Controllers are the entities who determine how personal data is processed. Processors are their vendors who process the personal data on their customers' behalf. The GDPR may apply to any entity who meets the GDPR applicability requirements contained within article 3. This article states that it "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union" even though where the processing takes place is immaterial. This article continues with the applicability of the GDPR to controllers or processors which are not located in the EU if they engage in certain data processing activities: "the offering of goods or services . . . to such data subjects in the Union" or monitoring the behavior of data subjects in the EU if such behavior "takes place within the Union" (2018). Therefore, the triggers for entities being subject to GDPR revolve around location of the entity and the data subjects. When GDPR was first adopted, there was a common fear that having one person from Europe engage in business, such as walking into a hospital in the United States, would then require the hospital to become GDPR compliant. Such is not the case. The company doing business must proactively engage in doing business in Europe. For example, having a website that is universally available does not necessarily bring an entity or an activity under the GDPR. However, if that website translated its terms to European languages or allowed a person to check out using European currency, those could be interpreted as proactively doing business in Europe (European Data Protection Board 2018).

In addition, the GDPR does have very strong data protection terms, many of which center around individual rights and principles of fair information practices. Individual rights are not a new concept, HIPAA has provided for individual rights since 1996. However, given the scope

and the breadth of the GDPR, this would certainly make individual rights a more mainstream concept than it had been so far. In addition, the GDPR added in the right of deletion, known as the right to erasure. This right in particular is something that worried a lot of businesses, especially those in the United States, given the propensity in the United States to maintain data for much longer than data is necessarily needed for the processing activity (Kerry 2018). The GDPR also has a 72-hour reporting period for data breaches. It defines a "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" (GDPR, article 4.12). Further the GDPR requires data protection impact assessments to be performed when there is a high risk to data, such as when special categories of data are processed, and that companies must maintain records of data processing. All of these concepts are new to most Universities, who up until now were able to manage FERPA in the student records department, GLBA in the finance department, and HIPAA in the medical centers. Omnibus privacy is not how the United States has traditionally managed personal data.

In addition to the Fair Information Practice Principles, such as data minimization, transparency and notice, purpose limitation, and security of personal data, the GDPR also added requirements around sharing data to third parties. Third parties that are engaged to do business on behalf of the company (the controller) are known as processors and any businesses they then contract are known as sub-processors. These relationships require very specific contractual requirements to be in place. If the data is going to cross international borders, for example out of the EU to the United States, then companies must put in a data transfer mechanism. These mechanisms vary between standard contractual clauses to binding corporate rules to codes of

conduct to an adequacy determine for the country where data is processed. The intent of this paper is not to get into the details of the complexities of international data transfer mechanisms, especially between the United States and the EU; however, one should be aware that this is a topic of consequence at this time between the two international powers. In addition, a data transfer is not merely the physical transportation of data across a border in a computer or on a drive, a transfer can also be a person in the United States accessing data that is stored in the EU or a person in the EU sending their data to a company in the United States (or any other country outside the EU).

The penalties for violating the GDPR can be quite steep. Corporate executives tend to be worried about the possibility of fines of up to four percent of global revenue, however we have not seen many penalties reach that level. The highest penalty assessed under GDPR at this time is €746 million by the Luxembourg data protection authority (*Commission nationale pour la protection des donées*) against Amazon Europe Core S.à.r.l. (Amazon.com, Inc. 2021). For Amazon, that amounted to less than one day's worth of revenue (Amazon.com, Inc. 2021). Yet the consequence can also be that the company is not permitted to do business in Europe or with European data subjects. This has much more far-reaching consequences than a monetary penalty, but we have also not seen that level of enforcement at this time.

For universities, the GDPR can be quite significant. Quite a few GDPR have programs that are directed towards individuals in the EU. For example, universities may have exchange programs, study abroad programs, they may recruit research subjects out of Europe, they may recruit professors or speakers out of the EU. All of these activities would then be subject to the GDPR. Therefore, one question is whether or not Universities are compliant with the GDPR. As

a side note, this researcher attempted to do a project based on Universities' compliance with the GDPR but was unsuccessful due to the heightened sensitivity to a potential compliance infraction to a major global privacy law. This in itself demonstrates the importance of privacy compliance in Universities and how serious they take such compliance. It does not necessarily mean they are or are not compliant with the GDPR and the purpose of this inquiry is not to determine if any one particular University is compliant.

Of the sample Universities, 78% are subject to GDPR and include information about GDPR compliance in their publicly available materials. The complexity of managing GDPR compliance alongside personal data that may not have any compliance requirements apply to it is difficult to manage. Universities, like private businesses, need to determine if they're going to deploy a separate and distinct level of controls to data that falls under the GDPR. In essence, this means Universities would have two levels of controls across the personal data within their databases. Therefore, they would have to segregate out personal data from students in Europe from other personal data on students and personal data from employees in Europe from other employee information. It is not a simple manner to conduct a privacy program by deploying controls based on geography.

Yet, in certain circumstances, Universities may find it to their benefit to deploy two sets of controls. For example, with the right to deletion, if there is a significant business reason to be able to maintain data past its usability for the purpose for which it was collected, then it might be reasonable to only apply the right to deletion to that data which has a right to deletion. This is only one example for which Universities may decide to deploy different controls, but they need to assess all the requirements of GDPR against their data processing activities and make a

decision as to how they will proceed in managing all of the personal data across all of their systems.

In 2019, the Campus Computing Project presented statistics showing that only 80% of private Universities and 50% of public ones were compliant with the GDPR (Green 2019). Lopez further reports that:

> Many universities who felt an early sense of urgency around becoming GDPR compliant are now taking a "wait-and-see" approach—slowing their compliance efforts until they see fines levied against larger educational systems. Unfortunately, many U.S. schools still do not understand the impact that the GDPR will have on their enrollment, research, and business dealings with students, faculty, and staff who are either from the EU or doing work there. While many may feel they have come a long way towards GDPR compliance, the reality is they have just put a privacy statement on their website or perhaps enacted one or two of the simpler policies around GDPR. (Lopez 2019)

In 2020, the Future of Privacy Forum's Director of Youth & Education Privacy, Amelia Vance, also cautioned that "many U.S.-based institutions remain unprepared, despite the high stakes." For more detailed information on how the GDPR applies to Universities, please see "The General Data Protection Regulation: Analysis and Guidance for U.S. Higher Education Institutions" by Dr. Gabriela Zanfir-Fortuna of the Future of Privacy Forum (2020).

Other International Privacy Laws

Very few other international privacy laws have the impact in the import of the GDPR. However, the United Kingdom (UK) separated from the EU with the final separation effective June 30, 2021). The UK has its own version of the GDPR, which it had to integrate with its current data

protection act. So, the UK GDPR is nearly identical to the EU GDPR, the only difference is being where the EU GDPR makes references to member states, the UK does not have member states, so it changed the language to reflect that difference. This means that where Universities need to account for GDPR compliance, they also need to account for the UK's GDPR. The considerations are essentially identical, but compliance measures need to be in place for each. For example, companies need to appoint a representative in the EU if the lack a physical presence (article 27). If that representative was appointed in the UK, then with the UK separated from the EU, the companies now need to appoint another representative in the EU. The converse is also true. If a representative was appointed in the EU, that person no longer qualifies as a representative for the UK. This could impact Universities subject to the GDPR.

Switzerland, who also invalidated its privacy Shield agreement with the United States on the heels of the decision in Schrems II (*Facebook Ireland v Data Protection Commissioner and Maximilian Schrems* 2020) by the Court of Justice of the European Union, issued its own guidance about international data transfers. Entities that need to implement standard contractual clauses as a cross-border transfer mechanism now have guidance on how to use the standard contractual clauses for Switzerland purposes.

China just passed its personal information Privacy Law (PIPL) which is effective on November 1, 2021. It also has extraterritorial provisions, and it has a potential fine of 5% Global revenue for companies who violate PIPL. The EU had a relatively slow ramp-up to enforcement activities, which is not expected to be the case for PIPL enforcement. However, like the GDPR, PIPL applies to data processed on individuals within the national borders of China. This would apply to residents of China while they're in China as well as visitors to China while they're inside

the national borders. There are a lot of similarities between the GDPR in PIPL, but University should know that there are also notable differences. One of the main differences being that there is no legal basis for legitimate interest available. Also, individuals have even more control over their data given the lack of this legitimate interest basis, meaning there will be a lot of data processed on the basis of consent. Consent is difficult to manage given that whenever there is a provision requiring consent there must also be a provision to revoke consent in a convenient and simple manner as which it was given in the beginning. In addition, there is a right for data deletion like the GDPR, but companies have a proactive requirement to delete personal data once it has exhausted the purpose for which it was collected or there is no legal reason to retain the data. Universities who may be subject to PIPL need to be paying attention to the requirements in an urgent manner given the penalties and enforcement. Also, like the GDPR, one of the consequences can be the restriction of doing business in China.

In addition, individuals who are responsible for processing the data, like senior management, executives, data protection officers, and privacy officers, may also be held personally accountable—facing fines, potential jail if it is a criminal violation, and the restriction of holding a position of processing data as it pertains to China. The enforcement of such a provision may be a little difficult to enforce depending on the exact circumstances, but that shouldn't impact the seriousness for which Universities consider their subjectivity to and compliance with PIPL. Of the sample Universities, 67% have established facilities in China or partnerships with China for various engagements and research. Does compliance with PIPL should be very high on the radar for them at this time.

5.3 Functional Areas of Privacy Law

Aside from the specific laws covered above, the remaining laws were functional areas of law. These ten laws comprised two identifiable sets of laws. The first set of laws relate to the Fair Information Practice Principles, such as limited sharing and data retention. The second set of laws are specific to activities or sectors of law, such as health and related laws and consumer protection laws. This results in the two groupings of laws as seen in Table 25, where the first grouping is the Fair Information Practice Principles laws, and the second grouping are more specific subject laws. Each of these are addressed in more detail.

Table 25: Grouping of Laws

Group 1	Group 2
Fair Information Practice Principle-related laws	**Subject-specific laws**
Limiting sharing / access laws / requirements	Consumer protection laws / requirements
Security laws / requirements	State privacy laws
Data retention laws / requirements	Health and related laws / requirements
Website privacy laws and notice requirements	Breach notification or reporting laws / requirements
Data minimization laws / requirements	Biometric laws / requirements

Fair Information Practice Principles

The fair information practice principles (FIPPs) are concepts pulled together across privacy laws and practices across the globe over decades. The same concepts are commonly found in most of the global privacy laws as well as the U.S. privacy laws. As seen in more detail in Table 26, the

eight FIPPs are Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness / Transparency, Individual Participation, and Accountability.

Table 26: Fair Information Practice Principles

1. Collection Limitation Principle	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. Data Quality Principle	Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.
3. Purpose Specification Principle	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use Limitation Principle	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except a) with the consent of the data subject, or b) by the authority of law.
5. Security Safeguards Principle	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. Openness Principle	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual Participation Principle	An individual should have the right: a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b. to have data relating to him communicated to him, within a reasonable time, at a charge, if any, that is not excessive; in a reasonable manner, and in a form that is readily intelligible to him; c. to be given reasons if a request made under subparagraphs (a) and (b) is denied and to be able to challenge such denial; and d. to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended;
8. Accountability Principle	A data controller should be accountable for complying with measures which give effect to the principles stated above.

(adapted from International Association of Privacy Professionals 2021).

Reviewing these FIPPs, one can readily identify the common concepts that were discussed above in the specific privacy laws. This explains why privacy experts would highlight these laws as opposed to specific laws, given that encompassing these concepts provides for a range of laws around the world that Universities may be subject to rather than listing specific laws. These also speak to the program elements that the Experts identified as necessary for a successful privacy program. Implementing these principles should form the foundation of a privacy program. Building a privacy program around principles or a framework creates consistency and provides entities with the flexibility to incorporate new laws or new guidance into an existing framework. For example, the Experts listed designating a person in charge of the privacy program as a critical element. Nearly all privacy regimes require a designated privacy program, including HIPAA, GDPR, and PIPL. Thus, building this element into a fundamental program design would accommodate legal requirements. This makes compliance a lot more manageable as opposed to being reactive towards changing circumstances and environments. Simplicity breeds consistency. Consistency breeds compliance. Compliance breeds trust.

Returning to the discussion above under GDPR, it is difficult enough to manage one successful privacy program much less a privacy program with different controls that react to different privacy laws. On a practical level, educating staff on managing student personal data is quite the ongoing effort. If that staff has to take additional steps to identify specific rules that apply to different students based on where those students may live or be located, it introduces an increasing amount of complexity into an already complex undertaking.

Subject-Specific Laws

The second category of subject specific laws comprises laws related to consumer protection, health and related laws, breach notification or reporting laws, biometrics, or state privacy laws. As mentioned above, the United States is unique in its approach to privacy. Laws from other countries typically address privacy in a general fashion and not on a sectoral basis. Therefore, subject specific laws are essentially state laws, although there are federal laws on some of these same topics. All states within the United States have consumer protection laws and breach notification laws. There are unique differences among the states in each of these categories, and the details will not be provided in this paper. In general, privacy notices do not address consumer protection laws or breach notification laws. Universities tend to have more policies related to security, as security imperatives have been around for decades, such as the payment card industry data security standards (PCI DSS). According to the Campus Computing Project, in 2019, all Universities reported being 100% compliant with PCI DSS. PCI DSS are not laws. PCI DSS are standards passed by the payment card industry, such as Visa and MasterCard, to require baseline security standards to be in place for companies to accept payments by credit cards.

Health and health-related laws on a state basis are quite prevalent. The exact topics may not be what the Experts had in mind when they considered that Universities need to comply with health and health-related laws, but health and health-related laws go beyond HIPAA. Specifically, states enact laws that must operate alongside HIPAA. California has the California Confidentiality of Medical Information Act and Texas has its Medical Privacy Act. According to the Health Information Law Project, twelve states have laws stronger than HIPAA related to patients accessing medical records and three have implemented medical record access laws for

entities not subject to HIPAA (2013). Given that one state with stronger laws is California, the sample population was impacted as two of the Universities were part of the University of California system. The remaining states are covered by HIPAA only.

In addition, almost all states have regulations on health information, whether this is who physicians or medical facilities may release information to, special reporting provisions for certain diseases or activities, or who owns medical records—all of which speak to privacy issues (Health Information & the Law Project 2021). For biometrics, the oldest state law is the Illinois Biometric Information Privacy Act of 2008 (BIPA, 740 ILCS 14/1 et seq.). This was soon

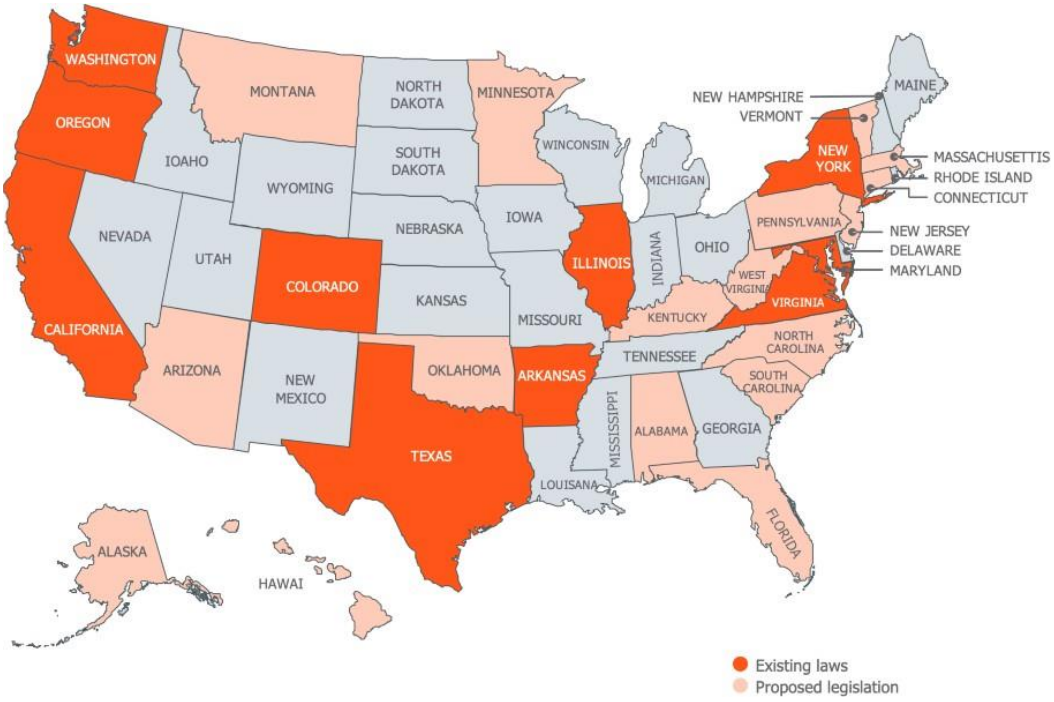


Figure 16: U.S. States with Biometrics Laws

followed by Texas, Washington, New York, and Oregon (de la Lama 2021). See Figure 16 for a map of the current and proposed state biometric laws and Appendix D for the full compilation (de la Lama 2021). This map and the referenced present both biometric laws alongside laws that include biometrics within the laws. Only Illinois, Texas, Washington, New York, and Oregon have specific laws on the use of biometrics.

State omnibus privacy laws were discussed in Chapter 2, but California is the only state with an active law, whereas Colorado and Virginia have both passed laws that will be effective in 2023. Over the past two years, multiple states have introduced privacy laws. Currently, six states have privacy bills in committee: Massachusetts, Michigan, New York, North Carolina, Ohio, and Pennsylvania (Royal 2021). As TrustArc explains;

> One of the complicating factors to understanding U.S. law is that the states all have different legislative sessions. Most states, 46 of them hold regular legislative sessions annually, with 22 states having "carryover" sessions from odd-numbered years to even-numbered years. This means in an odd-numbered year, like 2021, the bills that do not progress are carried over to the next year. The District of Columbia also does carryovers, sometimes called two-year sessions. Four states—Montana, Nevada, North Dakota, and Texas—meet in odd-numbered years. In addition, some states have full-time legislators, and the sessions are held the entire calendar year (with breaks) while others only have active sessions for part of the year—ranging from 30 to 120 days. Even further, most states allow for special sessions outside the standard legislative session (2021).

This complicates the review of state privacy laws, as not all bills which do not pass one year are "dead." Please see Figure 17 from the International Association of Privacy Professionals for an

excerpt from their State Privacy Legislation Tracker (2021). Please see Appendix C for the full chart. This chart shows the state bills that are still active, along with the consumer rights contained within the bill and the business obligations.

State	Legislative Process	Statute/Bill (Hyperlinks)	Common Name	Consumer Rights								Business Obligations				
				Right of Access	Right of Rectification	Right of Deletion	Right of Restriction	Right of Portability	Right of Opt-Out	Right Against Automated Decision Making	Private Right of Action	Opt-in requirement age	Notice/Transparency Requirement	Risk Assessments	Prohibition on Discrimination (exercising rights)	Purpose/Processing Limitation
LAWS PASSED (TO DATE)																
California		**CCPA**	**California Consumer Privacy Act (2018; effective Jan. 1, 2020)**	**x**		**x**		**x**	**x**		**L**	**16**	**x**			**x**
California [I]		**Proposition 24**	**California Privacy Rights Act (2020; effective Jan. 1, 2023)**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**L**	**16**	**x**	**x**	**x**	**x**
Colorado		**SB 190**		**x**	**x**	**x**		**x**	**x**	**x~**		**s**	**x**	**x**	**x**	**x**
Virginia		**SB 1392**	***Consumer Data Protection Act**	**x**	**x**	**x**		**x**	**x**	**x**		**13**	**x**	**x**	**x**	**x**
ACTIVE BILLS																
Massachusetts		SD 1726	Massachusetts Information Privacy Act	x	x	x	x	x	in	x	x	all	x		x	x
Minnesota		HF 1492	Minnesota Consumer Data Privacy Act	x	x	x		x	x	x		s	x	x	x	x
New York		A 680	New York Privacy Act	x	x	x	x	x	in	x	x		x			x
New York		S 6701	New York Privacy Act	x	x	x	x	x	in	x	x		x			x
New York [II]		A 6042	Digital Fairness Act	x		x		x	in	x	x	all	x	a	x	x
New York [II]		SB 567		x			x		x		x	x	x		x	
North Carolina		SB 569	Consumer Privacy Act	x	x	x		x	x	x~	x	s	x	x	x	x
Ohio		HB 376	Ohio Personal Privacy Act	x		x		x	x			13	x		x	x
Pennsylvania		HB 1126		x		x			x		L	16	x		x	

Figure 17: IAPP State Privacy Legislation Tracker

In general, and by necessity, state laws are triggered by doing business in the state, which does mean there needs to be a physical presence. Merely doing business with the residents is enough, in conjunction with some qualifying measure, such as the amount of data or revenue.

This does mean however that universities who qualify under state law are able to easily identify whether or not they qualify under state law, exactly like they would determine if they were subject to an international privacy law. The complicating factor is that now the United States with its move towards state omnibus privacy laws in the absence of a federal privacy law will start to resemble the EU under Directive 95, where each Member State had its own privacy law. As discussed above, this made it very complex for entities doing business across Europe to be able to comply with all privacy laws. With three state privacy laws on the books, it is unknown how many state laws it will take before the United States passes a federal omnibus privacy law. There have been multiple bills proposed yet each one fails for a variety of factors, the most common factors being debate over a private right of action and preemption of state law. (see in general, (International Association of Privacy Professionals 2021; TrustArc 2021). Of the sample Universities, 45% were subject to state privacy laws, e.g., the CCPA. Given that two are California Universities, only 22% were subject to state laws outside their own state.

A key consideration for the triggers of state privacy laws is the revenue consideration. California has clarified that it is not revenue from California business that triggers the California law, it is overall revenue that triggers the California law. Colorado and Virginia followed the same formula. Revenue is not the only trigger; however, revenue may be the primary trigger for Universities in considering their subjectivity to other states' laws. Typically, the trigger for the amount of personal data processed is based on the number of that states' residents that the Universities process. Therefore, revenue becomes a major consideration. On that point, California does exempt nonprofit institutions from the CCPA, but 50% of the sample

Universities in the private, nonprofit category included CCPA in its policies and public information.

5.4 Chapter 5 Summary

This chapter applies the law to the Universities, considering the results of the Document Analysis of Chapter 4 and the priorities identified by the Experts in Chapter 3. Given the complexity of privacy law and the complexity of Universities, it is inevitable that Universities are facing a complex undertaking in implementing and managing a comprehensive privacy program across all of the data subject, activities, applicable law, and risk factors. Further complicating the endeavor is how privacy law is established in the United States, especially with the new state privacy laws coming into effect. Universities have the same privacy laws to manage as private corporations do without seeing the same return on investment. Privacy is a cost center. But the lack of privacy carries a larger cost in terms of enforcement, reputation, breaches, and inability to engage in certain activities.

CHAPTER 6

CONCLUSION AND DISCUSSION

This chapter discusses the findings of the research as a whole and what they indicate for privacy compliance at Universities. It begins with a discussion of the findings in terms of the research questions followed by a discussion of the significance and implications of the study. Next, it presents the limitations and potential for future research. Lastly, it summarizes the key findings and offers concluding thoughts for privacy practitioners at Universities and how this line of inquiry may impact their programs.

6.1 Summary of Findings and Study

The literature review elicited that this topic is ripe for research given the scattered literature in existence on various aspects of privacy at Universities yet very little on overall privacy management at Universities. The underlying theory relies on Complexity Theory, both in privacy law as a complex adaptive system itself, layered on top of the well-established complexity of Universities. Within this, the implementation of public policy was also considered given the looming criticality of privacy compliance and the susceptibility of Universities to public involvement and oversight as well as their need to attract customers to remain financially stable and operational.

Following this research into the state of the market and scholarship, the methodology was designed. The state of privacy law has grown significantly within the past two years and the challenge was to take a snapshot in time of compliance, but as it spanned the past year, accounting for sensitivity to potential issues of noncompliance, in a rapidly emerging field. This research began with the premise that to best understand how Universities are managing privacy,

the parameters of whether Universities need to manage privacy needs to be established. To ensure the academic rigor of the undertaking, a Delphi method was used comprising global privacy professionals, over three rounds including of successive upvoting of critical factors. This method was presented in Chapter 3 and resulted in identifying the triggers for privacy laws, the most critical privacy laws that apply to Universities, and factors for success and risk.

The results of the Delphi method were that all Experts agreed that managing privacy compliance was complex, ranging from somewhat complex to very complex. On the topic of how well Universities were managing privacy, 80% of the Experts placed them in the somewhat ineffective to somewhat effective range, with an additional 12% ranking them as very ineffective. For the substantive upvoting segments, the factors addressed include the data subjects and activities that trigger privacy laws, the most important privacy laws applicable to Universities, the program elements that Universities need in their privacy programs, and the risk factors that Universities face that contribute to noncompliance with privacy laws.

The data subjects that trigger privacy laws are numerous: students, staff (employees, contractors, applicants, directors/regents), families (including both parents and dependents), visitors, guest speakers, patients, vendors, research subjects, customers, alumni, donors, faculty, members of the public (from website visitors to event attendees), payors of student fees, locale-based individuals including those from other countries, and people with disabilities. These data subjects were identified in Round 1 and not included in the upvoting due to the ubiquitous nature of these data subjects in general on college campuses. Along with the triggering activities below reiterates that Universities and privacy professionals need to be aware of what data subjects are

involved on campus. To determine if the Universities are subject to privacy laws, these data subjects need to be evaluated in context of the activities in which they are implicated.

The activities that trigger privacy laws are health-related activities, student administration, human capital management / employment, vendor management; data (analytics, capture, control, processing, retention); admissions, finance, activities and events, counseling; and law enforcement / policing / security and surveillance. As seen throughout the study, privacy laws are not just triggered based on the type of entity, they are triggered based on the data subjects and activities in which the Universities engage. Laws often have exceptions, but one must first identify the law that is triggered, then document an exception, if applicable. The privacy laws that are most critical to Universities are specific laws (FERPA, HIPAA, GDPR), laws based on FIPPs (e.g., transparency and data minimization laws), and subject-matter laws (e.g., biometrics and breach notifications).

The final two areas of evaluation were the programmatic elements that should be present along with the risk factors that may prevent Universities from being compliant with privacy laws. The program elements that Universities must have to be successful at managing privacy compliance are privacy program development and implementation; Chief Privacy Officer (CPO) / privacy lead designated; third party management); data security policy and program; dedicated staff with appropriate resources; training; privacy policies and procedures; central oversight; incident response process; and monitoring, audit, assessments. Combined with the risk factors, privacy professionals at Universities have a thorough checklist to follow to inform the design or enhancement of a privacy program. The risk factors Universities face are decentralized and siloed data systems; inadequate funding for data protection programs; lack of leadership focus

and evangelization of data privacy as a priority; existence of sensitive and confidential information in abundance and breadth; lack of a compliance culture; lack of awareness of laws and policies; extremely diverse activities, data sets, and data subjects; lack of employed or contracted staff that understand privacy; poor data protection controls; the huge number of sectoral activities; and outdated systems.

The results of the Delphi method were used in the Document Analysis, presented in Chapter 4. Using the top three to five factors in each section, the sample Universities were reviewed for these factors. The sample Universities comprised the top two (or three) ranked Universities along with two randomly selected Universities in both the public and private nonprofit sectors, with the theory that there may be a notable difference between top-ranked institutions and randomly selected not top-ranked institutions. This theory proved to be true. As presented in Chapter 4, most of the Universities have the data subjects that would trigger privacy laws, with some differences noted in activities, such as having student medical centers or research facilities. The presence of programmatic elements was difficult to ascertain in detail, but it was noted that not all Universities have defined privacy programs or designated privacy officials with the exception of someone who manages FERPA inquiries. Likewise, the presence of risk factors was difficult to assess without more research, but elements such as a lack of leadership evangelizing privacy was notable in its absence.

Lastly, the results of the Delphi and Document Analysis were then carried into the Doctrinal Legal Research in Chapter 5. Building on the fundamentals of privacy law presented in Chapter 2, the Doctrinal Legal Research took the laws as identified in the Delphi and assessed

the findings of the Document Analysis against the current laws, including any significant legal findings that included Universities, such as prevalence of HIPAA enforcement action.

After these efforts, what is the answer to the research question: "How are Universities in the United States managing compliance with privacy and data protection laws?" The answer—through complexity. The pandemic brought privacy issues to the forefront and Universities had to manage issues that were heretofore not even on the radar. Like most other businesses, Universities had to deploy thousands of remote offices and stay in business while protecting data in unknown environments. Not a simple undertaking at the best of times, much less in the perhaps worst of times. At the same time, new privacy laws are being developed, such as the Colorado Privacy Act, the China Personal data Protection Act, and the EU-U.S. Privacy Shield being invalidated. It's complicated.

6.2 Significance and Implications

This study seeks to enliven a discussion about privacy compliance in Universities that, although is a topic of concern and conversation, is a quiet one being held in darkened hallways and half-empty conference halls. To manage privacy compliance, Universities have to manage organizational change even while compliance budgets are being cut and qualified privacy professionals are in demand. It is difficult for Universities to compete for talent with private corporations.

By providing evidence of the layers of complexity that must be navigated in a rapidly evolving field, this study supports further work in this realm. Too many believe that Universities

only manage FERPA.[8] They are unaware of the breadth and scope of privacy laws that apply, the triggering factors that are ubiquitous at Universities, and the knowledge, skill, and experience that are needed to manage compliance in such a nuanced and deeply complex environment.

These findings also support the clear need for more research engaging a much broader body of stakeholders with the ability to examine in detail the unique compliance activities at individual Universities and devise a consensus on what is effective and why. If it is not effective, then the methods should be assessed along with the risk factors identified by the Experts.

Although exploratory, the factors identified by the Experts serve as an initial framework for evaluating privacy programs and identifying potential points of failure. This study is not a comprehensive overview but should be used as a departure point for further work and discussions around privacy compliance in Universities and how privacy compliance programs should be approached and considered. Lastly, this study puts the complexity of privacy compliance in Universities into context. It is a highly sectoral, nuanced, and multi-layered field with a variety of evolving factors, one that, like many questions of privacy, centers on "humanistic problems encompassing questions of law, ethics, culture, and social and professional norms that cannot be resolved through pure technical solutions" (Hofman 2020, 308). Any University aiming for compliance in their privacy programs cannot take a check-the-box approach.

[8] This reflects statements made to the researcher personally over the course of many years and specifically in relation to this line of inquiry.

6.3 Limitations and Future Research

The approach taken in this study was a high-level surveillance with a small sample size and a design that prevented more in-depth analysis as a case study was explicitly avoided in order to reach across a broader population. Additional studies that involve more longitudinal case studies would yield a richer data set and increase the knowledge base by delving into more details on the organization of the privacy departments, the challenges and successes of their measures, and a thorough examination of the risk factors. Overall, this study was limited geographically to Universities within the United States. A more diverse geographical study would account for whether these same issues arise in other nations.

As discussed in Chapter 3, the Delphi method design limited the ability to track Experts across rounds, which may have yielded more participation and thus, more insight. It is not positive, as the very nature of this issue indicates that there is no way to determine if Experts did participate in more than one round. Although the remote character of the Delphi was beneficial, there are additional steps that could be added to increase the ability for Experts to interact and clarify certain items. However, this can only be done in a way to prevent strong personalities from dictating the outcome over quieter personalities who are just as experienced, but perhaps not as vocal.

6.4 Benefits to Practitioners

One goal of this study was to yield practical results that would assist privacy practitioners at Universities to implement or improve their privacy programs. Although esoteric in nature, this goal was not lost during the process. By highlighting the complexity of the laws that apply to Universities, align with the factors within each, practitioners should have a more thorough scope

of how to determine if a law applies to them or not. Further, they are aware of the need to have certain knowledge and skills available to them to appropriately evaluate the applicability of laws. Plus, there is a basic framework provided by the Experts of data subjects and activities that trigger privacy laws, programmatic elements that should be built into a privacy program, the FIPPs, and risk factors to account for and possibly mitigate them with cross-functional cooperation and diligence.

6.5 Concluding Thoughts

This research is overdue. The educational field has had privacy law since 1974, rivaling the oldest privacy laws in the world. But FERPA has no teeth and seems uninclined to use its gums often. The U.S. Department of Education is understaffed and under-resourced to properly investigate FERPA violations. There are multiple FERPA violations that have never been reported for the sheer fact that nothing would really happen and if it did, it would be years down the road (personal knowledge of researcher). However, as demonstrated by this study, there are not only other privacy laws that apply to Universities, but the world of privacy law is also expanding tremendously. Universities manage the same privacy laws as private corporations, plus FERPA, and are not as equipped to do so. Privacy professionals at Universities do much of the same job for much less pay. It is time that they, both professionals and Universities, had significant resources and attention to manage privacy compliance in a stellar manner. Educause and IAPP do an admirable and well-respected job in how they are addressing these concerns. Think tanks, like the Future of Privacy Forum, are likewise issuing resources for educational institutions (Zanfir-Fortuna 2021). Hopefully, this study inspires more research and attention in this realm.

APPENDIX A

STATE CONSTITUTIONAL PRIVACY CLAUSES

State	Cite	Text
Arizona	Art. II, § 8	No person shall be disturbed in his private affairs, or his home invaded, without authority of law.
California	Art. I, § 1	All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.
Florida	Art. I, §§ 12 & 23	Section 12: Searches and Seizures The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated. Section 23: Right to Privacy Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.
Hawaii	Art. I, §§ 6 & 7	Section 6: Right To Privacy The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right. Section 7: Searches, Seizures and Invasion of Privacy The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures *and invasions of privacy* shall not be violated; and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized or the communications sought to be intercepted. [Am Const Con 1968 and election Nov 5, 1968; ren and am Const Con 1978 and election Nov 7, 1978]
Illinois	Art. I, § 6	Searches, Seizures, Privacy and Interceptions The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, *invasions of privacy or interceptions of communications by eavesdropping devices or other means*. No warrant shall issue without probable cause, supported by affidavit particularly describing the place to be searched and the persons or

		things to be seized.
Louisiana	Art. I, § 5	Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, *or invasions of privacy*. No warrant shall issue without probable cause supported by oath or affirmation, and particularly describing the place to be searched, the persons or things to be seized, and the lawful purpose or reason for the search. Any person adversely affected by a search or seizure conducted in violation of this Section shall have standing to raise its illegality in the appropriate court.
Montana	Art. II, § 10	The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.
New Hampshire	Art. 2-b	Right to Privacy. An individual's right to live free from governmental intrusion in private or personal information is natural, essential, and inherent.
South Carolina	Art. I, § 10	The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures a*nd unreasonable invasions of privacy* shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, the person or thing to be seized, and the information to be obtained.
Washington	Art. I, § 7	Invasion of Private Affairs or Home Prohibited No person shall be disturbed in his private affairs, or his home invaded, without authority of law.

APPENDIX B

STATE (AND D.C.) DATA BREACH NOTIFICATION LAWS

State	**Law**
Alabama	Ala. Code §§ 8-38-1 to -12
Alaska	Alaska Stat. § 45.48.010 et seq.
Arizona	Ariz. Rev. Stat. § 18-551 to -552
Arkansas	Ark. Code §§ 4-110-101 to -108
California	Cal. Civ. Code §§ 1798.29, 1798.82
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. §§ 36a-701b, 4e-70
Delaware	Del. Code Ann. tit. 6, § 12B-101 et seq.
District of Columbia	D.C. Code §§ 28-3851 et seq.
Florida	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)
Georgia	Ga. Code §§ 10-1-910 to -915; 46-5-214
Hawaii	Haw. Rev. Stat. § 487N-1 et seq.
Idaho	Idaho Code §§ 28-51-104 to -107
Illinois	815 ILCS §§ 530/1 et seq.
Indiana	Ind. Code §§ 4-1-11 et seq., 24-4.9-1-1 et seq.
Iowa	Iowa Code §§ 715C.1, 715C.2
Kansas	Kan. Stat. § 50-7a01 et seq.
Kentucky	KRS § 365.732, KRS §§ 61.931 to 61.934
Louisiana	La. Rev. Stat. §§ 51:3071 et seq.
Maine	10 Me. Rev. Stat. § 1346 et seq.
Maryland	Md. Code Com. Law §§ 14-3501 et seq., Md. State Govt. Code §§ 10-1301 et. Seq.
Massachusetts	Mass. Gen. Laws § 93H-1 et seq.
Michigan	Mich. Comp. Laws §§ 445.63, 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	Miss. Code § 75-24-29
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code §§ 2-6-1501 et seq., 30-14-1701 et seq., 33-19-321
Nebraska	Neb. Rev. Stat. §§ 87-801 et seq.
Nevada	Nev. Rev. Stat. §§ 603A.010 et seq., 242.183
New Hampshire	N.H. Rev. Stat. §§ 359-C:20, 332-I:5
New Jersey	N.J. Stat. § 56:8-161 to -166
New Mexico	N.M. Stat. §§ 57-12C-1 et. Seq.
New York	N.Y. Gen. Bus. Law § 899-AA
North Carolina	N.C. Gen. Stat §§ 75-60 et. seq., 14-113.20
North Dakota	N.D. Cent. Code §§ 51-30-01 et seq., 2021 H.B. 1314

Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1345.01 et seq.
Oklahoma	Okla. Stat. §§ 74-3113.1, 24-161 et seq.
Oregon	Oregon Rev. Stat. §§ 646A.600 to .628
Pennsylvania	73 Pa. Stat. §§ 2301 et seq.
Rhode Island	R.I. Gen. Laws §§ 11-49.3-1 et seq.
South Carolina	S.C. Code § 39-1-90
South Dakota	S.D. Cod. Laws §§ 20-40-19 to -26
Tennessee	Tenn. Code §§ 47-18-2107; 8-4-119
Texas	Tex. Bus. & Com. Code §§ 521.002, 521.053
Utah	Utah Code §§ 13-44-101 et seq.
Vermont	9 Vt. Stat. §§ 2430, 2435
Virginia	Va. Code §§ 18.2-186.6, 32.1-127.1:05
Washington	Wash. Rev. Code §§ 19.255.010, 42.56.590
West Virginia	W. Va. Code §§ 46A-2A-101 et seq.
Wisconsin	Wis. Stat. § 134.98
Wyoming	Wyo. Stat. § 6-3-901(b), §§ 40-12-501 to -502

APPENDIX C

IAPPUS STATE LEGISLATION TRACKER

https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf

State	Legislative Process	Statute/Bill (Hyperlinks)	Common Name	Consumer Rights: Right of Access	Right of Rectification	Right of Deletion	Right of Restriction	Right of Portability	Right of Opt-Out	Right Against Automated Decision Making	Private Right of Action	Business Obligations: Opt-in requirement age	Notice/Transparency Requirement	Risk Assessments	Prohibition on Discrimination (exercising rights)	Purpose/Processing Limitation
LAWS PASSED (TO DATE)																
California		**CCPA**	**California Consumer Privacy Act (2018; effective Jan. 1, 2020)**	**x**		**x**		**x**	**x**		**L**	**16**	**x**			**x**
California [I]		**Proposition 24**	**California Privacy Rights Act (2020; effective Jan. 1, 2023)**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**L**	**16**	**x**	**x**	**x**	**x**
Colorado		**SB 190**		**x**	**x**	**x**		**x**	**x**	**x~**		**s**	**x**	**x**	**x**	**x**
Virginia		**SB 1392**	***Consumer Data Protection Act**	**x**	**x**	**x**		**x**	**x**	**x**		**13**	**x**	**x**	**x**	**x**
ACTIVE BILLS																
Massachusetts		SD 1726	Massachusetts Information Privacy Act	x	x	x	x	x	in	x	x	all	x		x	x
Minnesota		HF 1492	Minnesota Consumer Data Privacy Act	x	x	x		x	x	x		s	x	x	x	x
New York		A 680	New York Privacy Act	x	x	x	x	x	in	x	x		x			x
New York		S 6701	New York Privacy Act	x	x	x	x	x	in	x	x		x			x
New York [II]		A 6042	Digital Fairness Act	x		x		x	in	x	x	all	x	a	x	x
New York [II]		SB 567		x			x		x		x	x	x		x	
North Carolina		SB 569	Consumer Privacy Act	x	x	x		x	x	x~	x	s	x	x	x	x
Ohio		HB 376	Ohio Personal Privacy Act	x		x		x	x			13	x		x	x
Pennsylvania		HB 1126		x		x			x		L	16	x		x	
FAILED BILLS																
~~Alabama~~		~~HB 216~~	~~Alabama Consumer Privacy Act~~	x		x		x	x			~~18~~	x		x	x
~~Alaska~~		~~SB 116~~	~~Consumer Data Privacy Act~~	x		x		x	x			~~18~~	x		x	x
~~Arizona~~		~~HB 2865~~		x	x	x	x	x		x			x	u		x
~~Connecticut~~		~~SB 893~~		x	x	x		x	x				x	x	x	x
~~Florida~~		~~SB 1734~~	~~Florida Privacy Protection Act~~	x	x	x			x	x		~~18~~	x		x	
~~Florida~~		~~HB 969~~		x	x	x		x	x		x	~~16~~	x		x	x
~~Illinois~~		~~HB 3910~~	~~Consumer Privacy Act~~	x		x		x	x			~~18~~	x	x	x	x
~~Kentucky~~		~~HB 408~~							x			~~16~~	x		x	
Maryland		SB 0930	~~Maryland Online Consumer Protection Act~~	x		x		x	x				x		x	
~~Minnesota~~		~~HF 36~~		x		x		x	x		x	x	x		x	
~~Mississippi~~		~~SB 2612~~	~~Mississippi Consumer Privacy Act~~	x		x			x		x	x	x		x	
~~North Dakota~~		~~HB 1330~~							in		x		x			
~~Oklahoma~~		~~HB 1602~~	~~Oklahoma Computer Data Privacy Act~~	x		x			x			~~all~~	x		x	
~~Texas~~		~~HB 3741~~		x	x	x		x					x			x
~~Utah~~		~~SB 200~~	~~Consumer Privacy Act~~	x	x	x			x	x	x	s	x	x	x	x
~~Washington~~		~~SB 5062~~	~~Washington Privacy Act 2021~~	x	x	x		x	x	x		x	x	x	x	x
~~Washington~~		~~HB 1433~~	~~People's Privacy Act~~	x	x	x	x	x	in		x	x	x		x	x
~~West Virginia~~		~~HF 3159~~		x	x	x		x	x		x	~~16~~			x	x

In Session: all above states

Introduced > In Committee > Crossed Chamber > Cross Committee > Passed > Signed

Bold - passed law
~~Strikethrough - bill died in committee or postponed~~
* Continued to 2021 Special Session

L - private right of action for security violations only
in - opt-in consent requirement
p - prohibition without consent
u - unclear
s - opt-in requirement for all sensitive data
a - risk assesment limited to impact of automated decisions
~ - right to opt out of certain automated decisionmaking

[I] California Privacy Rights Act's right of restriction/limitation is only applicable to sensitive personal data
[II] Companion bills introduced at different time during legislative session

Legislative Process: Introduced > In Committee > Crossed Chamber > Cross Committee > Passed > Signed

Further information and most recent version of the IAPP's US State Comprehensive Privacy Law Comparison can be found here.

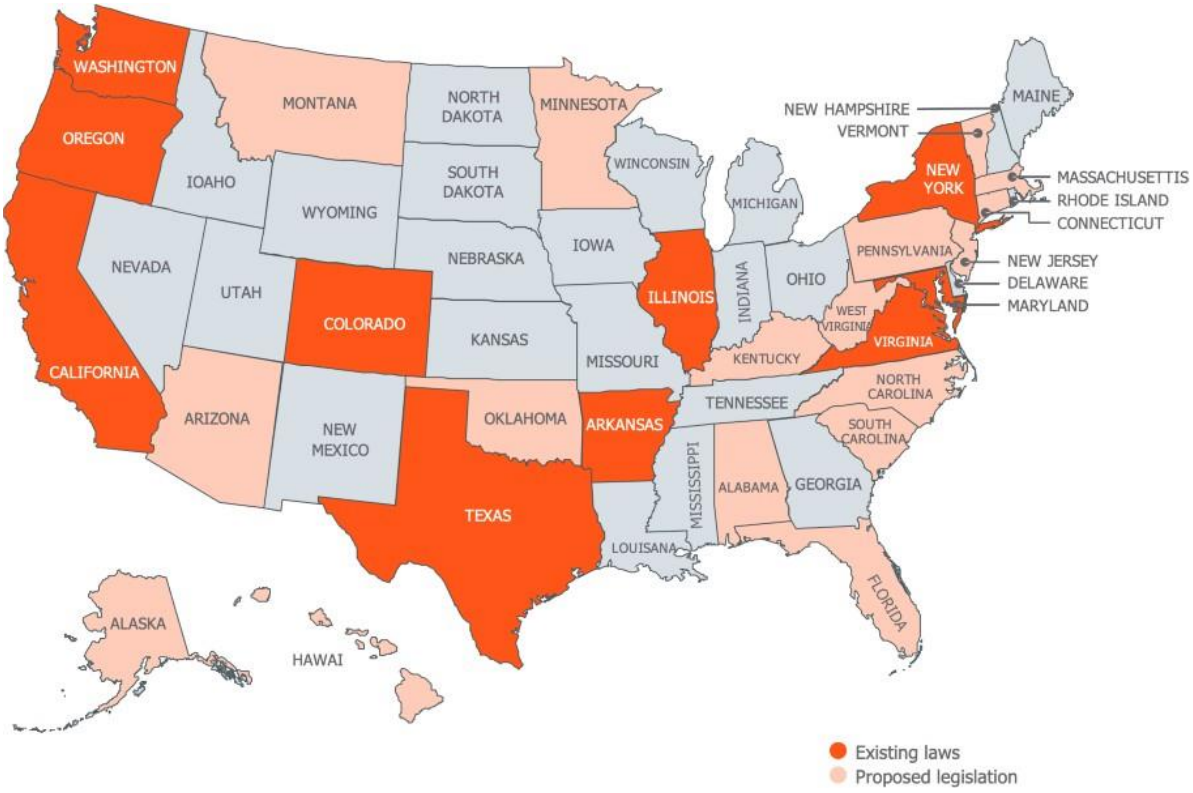
iapp

Last updated: 9/16/2021

APPENDIX D

U.S. BIOMETRIC LAWS

By Amy de la Lama of Bryan Cave Leighton Paisner
(last updated May 12, 2021)
Reprinted with the permission of Bryan Cave Leighton Paisner
LOCATED AT https://www.bclplaw.com/print/content/1032671/US-Biometric-Laws--Pending-Legislation-Tracker.pdf



Existing Laws- Excerpt

Arkansas	Personal Information Protection Act ("PIPA"); ARK. CODE. ANN. §§ 4-110-101 *et seq*.	Requires a business to take all reasonable steps to destroy or arrange for the destruction of a customer's records containing personal information (which includes "biometric data") and implementation and maintenance of reasonable security procedures and practices. Provides for enforcement by the Arkansas Attorney General.
California	California Consumer Privacy Act ("CCPA")	Comprehensive data privacy statute that includes obligation to make certain disclosures regarding collection of biometric data.
Colorado	Consumer Protection Act COLO. REV. STAT. ANN. §§ 6-1-713, 6-1-713.5	A covered entity that maintains, owns, or licenses personal identifying information (including biometric information) must develop and implement a written plan for the disposal of such information and must implement and maintain reasonable security procedures and practices.
Illinois	Biometric Information Privacy Act ("BIPA") 740 ILCS 14/1 *et seq.*	BIOMETRIC SPECIFIC. Depending on whether a private entity is possessing, capturing, collecting, otherwise obtaining, or disclosing biometric information or biometric identifiers, requires: (1) a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information; (2) compliance with that policy; (3) protection of the biometric information using the reasonable standard of care within the industry or in a manner as protective as the entity protects other confidential and sensitive information;
		(4) informing the subject whose biometric information is to be collected of the specific purposes and length of term for which biometric information is being collected, stored, or used; and (5) receiving a written release from the individual to proceed with the collection or disclosure of the biometric information.

		Provides for recovery of liquidated statutory damages or actual damages, and attorneys' fees and expenses.
Maryland	Personal Information Protection Act MD. CODE ANN., COM. LAW §§ 14-3501 *et seq.*	Requires a business to take reasonable steps to protect against unauthorized access to or use of personal information (including biometric data), including requiring in contracts with certain nonaffiliated third party service providers that the service provider will implement and maintain reasonable security procedures and practices.
New York	Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act")	Comprehensive data security statute that applies to biometric information. More information on the SHIELD Act can be found here.
New York	N.Y. LAB. LAW § 201-a.	BIOMETRIC SPECIFIC. Prohibits employers from requiring a fingerprint from employees, as a condition of securing employment or of continuing employment, unless as provided by other laws. (*See also* New York State Department of Labor RO-10- 0024 for opinion on use of a biometric device in a time clock).
New York	City of New York Administrative Code, Title 22, Chapter 12	BIOMETRIC SPECIFIC. Any "commercial establishment" that collects biometric information from "customers" must disclose the collection "by placing a clear and conspicuous sign near all of the commercial establishment's customer entrances." Makes it unlawful to sell, lease, trade, share, exchange for anything of value, or otherwise profit from the transaction of biometric identifier information.
Oregon	Portland City Code, Title 34- Digital Justice, Chapters 34.10.010-34.10-50	BIOMETRIC SPECIFIC. Prohibits the use of Facial Recognition Technologies in Places of Public Accommodation by Private Entities within the boundaries of the City of Portland. Provides for recovery of damages sustained as a result of the violation of $1,000 per day for each day of violation, whichever is greater.

Texas	TEX. BUS. & COM. CODE ANN. § 503.001	BIOMETRIC SPECIFIC. Requires that a person capturing a biometric identifier of an individual for a commercial purpose inform the individual before capturing the biometric identifier and receive the individual's consent and requires protecting the data from disclosure using reasonable care and in a manner as protective as the entity protects other confidential information. Biometric identifiers must be destroyed within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the biometric identifier expires. Also prohibits a person in possession of a biometric identifier of an individual from selling, leasing, or otherwise disclosing the biometric identifier unless in certain circumstances. Provides for a civil penalty of no more than $25,000 for each violation, enforceable by the Texas Attorney General.
Virginia	Virginia Consumer Data Protection Act	Comprehensive data privacy statute that includes obligation to obtain consent prior to collection or use of biometric data. Provides for civil penalties of up to $7,500 per violation, enforceable by the Virginia Attorney General. (Effective date January 1, 2023).
Washington	WASH. REV. CODE §§ 19.375.010 *et seq.*	BIOMETRIC SPECIFIC. Provides that a person may not enroll a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose. Provides for enforcement by the Texas Attorney General under the Washington Consumer Protection Act.

APPENDIX E

INFORMED CONSENT – ROUND 1

(SUBSTANTIVELY SIMILAR IN ALL ROUNDS)

Welcome to the "Privacy Compliance of US Universities," a web-based survey based on the Delphi method to survey privacy experts for important factors to consider in this topic. Before taking part in this study, please read the consent form below and click on the "I agree" button at the bottom if you are 18 years or older, understand the statements, and freely consent to participate.

Consent Form
This study involves a web-based survey comprising about questions. The survey is designed for privacy professionals in a series of **three surveys**, each one narrowing the topics based on the compilation of the responses in the prior surveys. The study is being conducted by K Royal (a PhD candidate) and Dr. L. Douglas Kiel of The University of Texas at Dallas and has been approved by the University of Texas at Dallas Institutional Review Board. No deception is involved, and the survey involves no more than minimal risk to participants (i.e., the level of risk encountered in daily life).

This first round may take 30 - 45 minutes to complete, but subsequent rounds will be much shorter. All are strictly confidential. Participants will be asked to respond to a series of questions about privacy / data protection activities at universities based on industry knowledge of privacy compliance. Each round will include three short demographic questions about general geographic location (in the United States or outside the United States), and knowledge of or experience in privacy laws applicable to universities or the United States. We do ask that you complete these three questions identically each round.

No specific experience in universities is required to participate.

Although all surveys are issued using an anonymous link, there is a possibility that you could be identified. The panel of experts will not be listed by name, but rather the demographics to identify the aggregate expertise of the panel will be included Answers will not be associated with individual respondents. The survey is issued through a tool called Qualtrics and is transmitted using https - a secure protocol over internet traffic, but there is a small possibility that responses could be viewed by unauthorized third parties (e.g., computer hackers). Responses are stored securely using a service called Box, a cloud storage provider, as well as on the researcher's personal device with care taken to prevent the proliferation of any identifying information.

The survey was tested, and no individuals reported adverse reactions during the test.

Participants are not being paid for responses. This is a completely voluntary activity. Refusal to participate involves no penalty or loss of benefits to which participants are otherwise entitled and participants may cease responding or withdraw at any time with no repercussions or consequences to the participants or their institutions.

If participants have any questions about this survey or the resulting analysis, they may contact the Principal Investigator, K Royal, at kroyal@utdallas.edu or Dr. L Douglas Kiel at dkiel@utdallas.edu. Participants who wish more information about their rights as a participant or want to report a research-related concern may contact The University of Texas at Dallas Institutional Review Board at (972) 883-4579.

Thank you in advance for your assistance in this research. **Please try to respond as soon as possible** so the group can move on to phase 2 quickly.

If you are 18 years or older, understand the statements and your rights as presented above, and freely consent to participate in the study, please click "I agree" below to begin.

APPENDIX F

SAMPLE RECRUITING MESSAGE

Email script as approved by IRB on Round 1

Hello. Hope you are well. I am doing my PhD dissertation on privacy complexities in universities. As part of the process, I will be using the Delphi method to narrow down the topics to focus on. This is a series of votes among a group of knowledgeable privacy professionals around the world to identify the critical issues in managing personal information at universities. I am aiming to have between 20 – 50 professionals participate. To increase the recognition of the validity of the process, I need the best people in the group of experts. Would you be willing to join the group, engage in a short series of votes and help me in this effort?

Names of participants will not be used. However, given that there is a small pool of professionals who will be participating, there is a small chance that you could be identified.

Your participation would be greatly appreciated.

Please let me know at your earliest convenience.

Thank you,
K

APPENDIX G

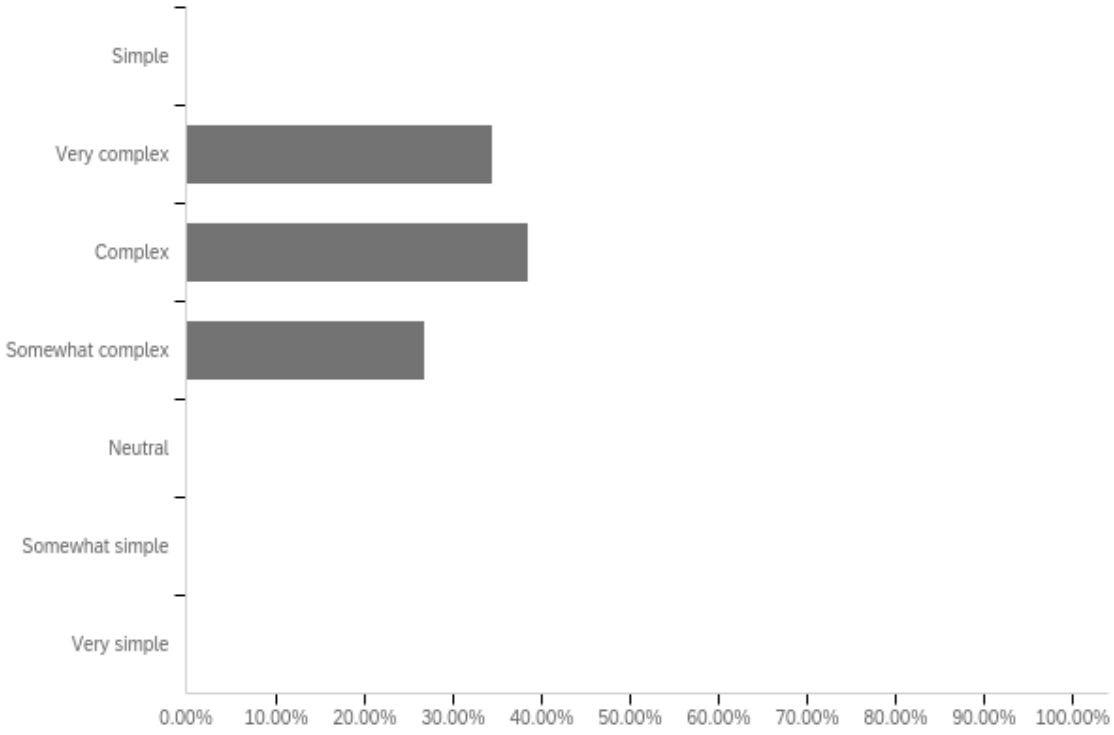
ROUND 1 INSIGHT AND SUBSTANTIVE RESPONSES

Privacy in US Universities

October 11th 2021, 6:58 pm CDT

Q1 - Please provide a response based on your professional judgment. Comments are allowed to explain where you feel necessary.

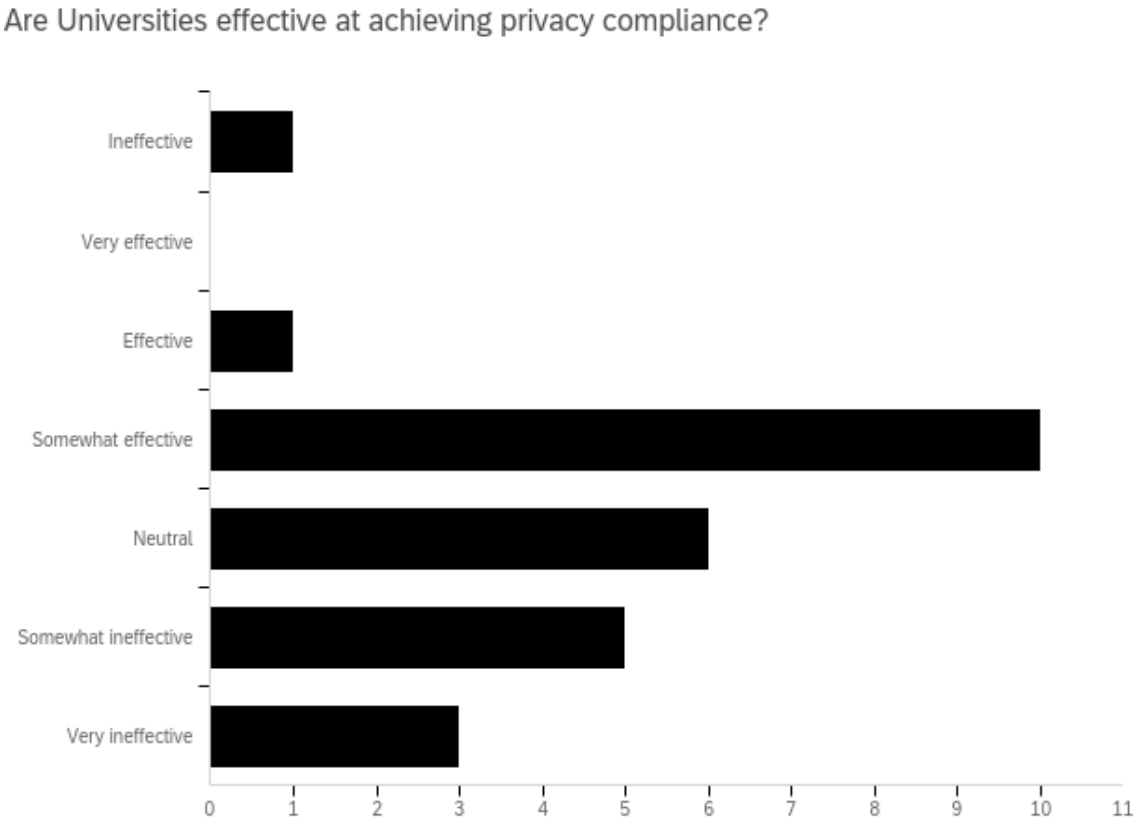
Is achieving privacy compliance at Universities simple or complex?



#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Do you believe that achieving privacy compliance at universities is simple or complex?	44.00	46.00	44.92	0.78	0.61	26

#	Answer	%	Count
1	Simple	0.00%	0
44	Very complex	34.62%	9
45	Complex	38.46%	10
46	Somewhat complex	26.92%	7
47	Neutral	0.00%	0
48	Somewhat simple	0.00%	0
49	Very simple	0.00%	0
	Total	100%	26

Q2 - Please provide a response based on your professional judgment. Comments are allowed to explain where you feel necessary.



#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Do you believe that most universities are effective at managing / achieving privacy compliance?	1.00	49.00	45.19	8.91	79.31	26

#	Answer	%	Count
1	Ineffective	3.85%	1
44	Very effective	0.00%	0
45	Effective	3.85%	1
46	Somewhat effective	38.46%	10
47	Neutral	23.08%	6
48	Somewhat ineffective	19.23%	5
49	Very ineffective	11.54%	3
	Total	100%	26

Q3 - What types of data subjects present at universities would trigger privacy laws?

students, faculty, foreign students, foreign faculties, research study participants, patients at university hospitals, alumni
Athletes, Faculty as employees, students, applicants, other university employees, potential students (which may be just considered general consumers for marketing purposes). Vendor and service provider contacts. Research participants. Patients for in campus medical clinics.
Students, exchange students, employees, dependents, professors, research subjects, patients, guest speakers,
Students, visitors (physical and virtual), employees
Students, faculty, employees, visitors, contractors
All. Students, faculty and staff, applicants, parents and other family members, alumni, visitors. Compliance is not just FERPA.
Students under 18 years of age, disabled, people from the EU or UK, California
Students, applicants, faculty, visitors, vendors, employees, event attendees, family members of students, and alumni
Students, employees, potentially patients and consumers
The term data subject is a little vague. In privacy that term often means a person who is the owner of personal data. But here I think it means types of data. Assuming that is correct, universities have health data, grade data, student output data, research data, even crime data, registration data, financial data.
Students, Employees, Research, Human Subject research
Students/applicants (FERPA)...Europeans (GDPR)...patients (e.g., university hospitals/health clinics - HIPAA) ...faculty/staff (employee privacy rights)
Don't understand the question
Students, employees
students (enrolled & applicants), teachers, website visitors, payors (of student fees), workforce (existing and applicants), research subjects, etc.
Employees, directors/regents, students, contractors (cafeteria workers, custodians/janitors, repair personnel); research participants/research subjects; unknown third parties
students, faculty, visitors, guests, applicantsemployees
Student, Faculty, Staff, guests
students, staff, contractors
students, staff, faculty, visitors/families, applicants, vendors, service providers
Students, Staff, Data Subjects participating in university research studies of various sorts (both internally facing and externally facing).

Students, employees, visitors, vendors, faculty, adjunct faculty, staff, contractors
Students, employees, applicants, donors, teachers, alumni, members of public, patients
Staff, patients, vendor personnel, students, research subjects, customers (as there is a large business tied to many bigger universities), alumni and donators, etc.
Students
Students, staff, parents, visitors

Q4 - What types of activities present at universities or that universities engage in would trigger privacy laws / standards?

Admissions of students from Europe or other countries that have comprehensive privacy law like Brazil; processing health data; hiring from Europe or other countries with similar privacy laws; online learning; international research projects
COVID related data and activities, Athlete health related tracking, Marketing to potential students, security monitoring, health research, student surveys, academic records, communication faculty to student etc., athlet
Education, exchange programs, lians, healthcare, taking payments by credit card, conferences, overseas locations
Education (in person and remote), healthcare, security or surveillance cameras, law enforcement, research
R&D, education, seminars/conferences
Instruction, admissions, billing & finance, fundraising, human resources, housing, health services, athletics, research. Basically all activities they engage in are likely to touch one or more privacy laws.
Selling products and services to students, Financial and health data capture
The entire lifecyle from application through graduation, including financial aid considerations, living situations, family member information, grades, employment, health care at student centers, financial information
Education, employment, advertising, commercial activities, research, healthcare
Certainly demographic, personal, health and finance info gathering and use and policing are the easy ones. Then there is intellectual property creation. Classroom, Registration, Policing, Medical, Activities/Events, Clubs. In some ways the university is the quenticential public square and privacy is not expected but there are certain data that the university gets that has or should have privacy requirements.
See Q.3
Data capture/control/processing; recordkeeping; administration (RTP).
admissions, finance, health, residence...too many to name
Health and payment related
Student registration, financial/fees, research, employment
Research, education, law enforcement, administration, application/payment, newly-minted "adults" who don't know what is acceptable yet
everything they do
Contact tracing, Student Analytics, research

communication infrastructure, course registration, research, tech transfer, counselling, teaching
applications, student/class lists, tuition payments/billing, student/faculty health services, faculty employment records, faculty salary payments, student/faculty housing, vendor management, fundraising efforts, university marketing/outreach, student athletic/activity participation
Student Administration Services, Student Records, Human Capital Management, Research conducted on behalf of other government entities and private entities.
Hard to answer without writing a book - there are hundreds of activities!
Grading; discipline; assessments; benefits, salary provision; financial support and scholarships; surveys; promotional activities; job placement; research and data analytics
Privacy is triggered in almost 90-95% of activities that any university does.
Healthcare/social
All involving personal data

Q5 - What privacy laws / requirements do you believe are important for universities to follow?

FERPA where applicable; GDPR where applicable; state laws and bills to the extent they can be applicable to universities; HIPAA for university hospitals?
All of them.
Ferpa, hipaa, common rule, pci, ccpa, gdpr, glba, state,
FERPA, HIPAA, CCPA/CPRA (in Ca), Biometric privacy laws, other state specific laws
It depends on where they are located, how the education/seminar/R&D is performed
FERPA, CCPA, HIPAA, certain research could involve various biometric and genetic privacy laws, billing and loan activity could involve FCRA and other financial privacy laws, state student privacy laws (most are limited to K-12, but I beleive some may affect universities), various emerging state consumer privacy laws, etc.
Data Minimization,linit data retention when possible
FERPA, CPRA, GDPR and other international data protection laws, consumer protection laws for websites, financial privacy and security laws, HIPAA (and state level health privacy laws such as CMIA), breach notification laws and others.
Depends on their activities- FERPA, FTC related, HIPAA, state laws, Part 2
The US doesn't have an omibus privacy legalisation, so the patchwork of various laws we do have apply to areas as health, finance, policing, IP related.
All applicable laws
All of them?
FERPA, State Laws
FERPA, HIPAA
Depends on where they are/where their constituents are... certainly FERPA, but also potentially CCPA, CPRA, GDPR, COPPA, etc.
It's a little flip to say "all of them", but all of them. The fact that you're a university does not mean that you don't have to be cognizant of the rules.
FERPA, HIPAA, GLB, Can-spam, COPPA
Is there an option to not follow the law? So all...
data safeguards
FERPA, HIPAA, CCPA, GDPR, state privacy laws

FERPA, CCPA, GDPR
There are numerous federal and state laws that universities must follow beyond FERPA.
Security of data, laws limiting sharing/access, breach, data transfer
It depends. Every state law is possible as well as international laws depending on the nexus of personal data being processed. HIPAA will definitely impact all universities as even the smallest has a campus health service acting as a covered entity.
HIPAA, possibly FERPA, PCI,
Any relevant jurisdictional privacy law and industry sector law.

Q6 - If you were to review universities for privacy compliance, what are the institutional and / or programmatic elements (in no particular order) you believe should be present?

data maps and records of processing activities, data protection impact assessments, general privacy policy and specific privacy notices for specific activities, data breach notification procedures, processes to reply to access, correction, deletion requests
I regular and consistent training for specific groups and activities to ensure awareness of privacy handling requirements. Information security review. Notice and external facing information review, internal data handling policy and practice review, training,
Notice, consent, breach response, Privacy officer, security, policies, individual rights, central oversight, audit, board reporting
IT, HR, Vendors (Saas and Cloud), Research publishing that involves datasets that may contain personal data, Admissions (especially use of AI or automated decisions), Notices (Policies),
An understanding of the kinds of information they have in their environment, including the data subjects, how/where the information is collected, whether the subjects expressly consented to the collection, data retention policies
Dedicated staff focused on privacy (with sufficient resources), awareness / compliance training for all faculty and staff who handle personal information, internal policies and procedures - including reviews of key operations that handle personal information, incident response procedures in the event of a data breach or other privacy incident.
There should be knowledge by all about their responsibilities related to data privacy
All collection points (applications), websites, grade reporting from professor records through the university level, information about dorm living, student health care, sign-ups for activities. There should be an overall policy that covers protection of student data from all points of collection, processing, access by others, through graduation. Alumni records, records of financial giving should also be addressed.
All elements of a compliance program
Every university should have a Privacy Officer who knows the vast majority (if not all) of sources of data that comes into the university which have regulatory risks and how they are complying to those obligations. This data map and registration of regulatory risk events and how they have remedied or mitigated the risk would be an important measure.
Governance, data classification, and handling matrix
Someone with institutional authority and responsibility for privacy; regular audits; good recordkeeping and data management; strong policy and procedures; mandatory training; breach procedures; assessment of third party services
Policies, complaint management, data security
Data inventories, DPIAs, HIPAA assessment
8 elements of an effective compliance program

Protection of student records; protection of employee records; understanding of rights of foreign citizens attending the University; protection of students in conflict with other students; policies/notices
all of them
A names person responsible for Privacy and/or Privacy Compliance
governance, privacy policy, data security policy, privacy breach mgmt
external privacy notices, internal privacy policies + procedures, staff privacy/security training, CPO or privacy director, PIA process, DSAR response process and staffing, incident (data breach,etc.) response process, privacy program development and implementation
Robust Data Governance program, Proactive Information Security Program, Consistent Data Privacy Education for all stakeholders.
Hard to answer without writing a book. Short answer: governance, training, assessment, policies, CPO
Policy and privacy notice; evidence of procedures to implement at departmental level; participation by departments in program; monitoring and audit
My first effort would be to thoroughly audit thier security controls as this is often an area of failure or resource gaps and can lead to sooo much more. Then training including, if was ever possible training students as staff. Both are a serious point of insecurity. Then I would review the vendor and partner management, including contracts. There is much more but those are often areas that I have seen need improvement.
Pick a framework and follow it.
Depends on jurisdiction. But would assess against own privacy programme maturity model.

Q7 - What are the risk factors at universities for noncompliance in terms of privacy compliance?

(THOSE ADDRESSING CONSEQUENCES ARE INDICATED IN GRAY)

automated admission screenings, indefinite retention times for all data, not being able to reply to data subject rights requests, weak security and many others
Extremely diverse activities, data sets, and data subjects. misinterpretations that newer privacy laws do not apply, information security/breach risk issues, meaningful informed consent for young adults Who may not be sophisticated, Data inventories and records of processing are likely nonexistent.
Non centralized privacy management, government run, lack of knowledge, massive span for both data subjects and laws, type of information held, outdated systems, employees who don't want to change
Probably limited, FERPA doesn't seem to have real enforcement consequences. HIPAA fines from HHS. Reputational damage.
Monetary damages, reputational risk, drops in enrollment, loss of funding
Lack of a compliance culture (e.g. faculty and staff who feel they have the autonomy to not follow established policies and procedures), lack of awareness of laws and policies (and the reasons behind them), decentralized and siloed data systems.
Fines, lack of trust, lower enrollment
Lack of overall security and privacy policies through the entire lifecyles, probably outdated storage requirements, lack of resources to focus on record retention, descturction, unclear level of responsibilities for various levels of data (i.e., dorm information and access to that information as an example).
Lack of employed or contracted staff that understand privacy and lack of resources generally
Risk factors include the existence not sensitive and confidential information in abundance and breadth; The likelihood or number of individuals with technical skills and likely limited professional maturity not to do something stupid. Universities hold info created about individuals during very formative years of an individual's life. Research on the cutting edge happens here, the confidentiality of which during creation can make or break future careers.
Not sure substantially different than other institutions
The huge number of sectoral activities at play in the average university
Government Funding Loss
Litigation, loss of trust
FERPA violations; state/fed/Intl law violations; reputational harm
Risk of harm to students if information is "leaked"; risk of harm to employees/educators if research is not properly managed/protected; risk of harm to human subjects of research; too many others to name
all of them
Aside from fines, loss of trust from campus community

poor data protection controls, introduction of new technologies
data breach, damage to reputation, lawsuits in some circumstances, declining enrollment
Ignorance of Privacy Law/Regulations, Lack of University Leadership focus & evangelization of Data Privacy as a priority, Adequate funding for data protection programs (privacy/security).
Violation of laws, failure to stop harm (Virginia Tech massacre, cyberbullying suicides), data breaches, and many other bad things.
Security breaches, fluctuating population, risk activities (e.g. file sharing), departments and professors acting on own judgment/ignore of policies, research activities gathering personal data, use of health/research data
Fines, business loss, reputations harm, etc.
Legal, regulatory, ethical, reputational and operational
Depends on jurisdiction. Regulatory Reputational and harm to individuals

APPENDIX H

ROUND 2 UPVOTED RESPONSES

Privacy in US Universities - Second phase

October 11th 2021, 6:55 pm CDT

Q4 - Out of the following activities present at universities or that universities engage in that would trigger privacy laws / standards, please select seven (7) that you feel are the most important / most common activities.

#	Answer	%	Count
4	activities and events (marketing, presenters, attendees, purchases, administration, online and remote, in-person)	3.57%	6
7	administration	2.98%	5
8	admissions (domestic and foreign)	7.74%	13
9	assessments	1.19%	2
10	athletic-related (assessments, health, performance, events)	2.98%	5
11	clubs	0.00%	0
12	commercial activities	0.60%	1
13	communications (students, staff, external, infrastructure)	0.00%	0
14	counseling	5.95%	10
15	data (analytics, capture, control, processing, retention)	8.93%	15
16	demographics	0.60%	1
17	education (in person and remote)	0.00%	0

18	exchange programs (students and faculty)	0.60%	1
19	family member information	2.38%	4
20	finance (billing, payment cards, collections, loans)	8.33%	14
57	fundraising	0.60%	1
58	health-related activities (research, student health, workers comp, health centers, occupational reporting, sick leave, insurance claims, reporting)	12.50%	21
59	hiring from Europe or other countries with similar privacy laws	0.00%	0
60	housing and living situations	0.60%	1
61	human capital management / employment (staff / faculty/contractors, applications, management, benefits, salary, contracts / contractors, performance reviews, student reviews, publications)	7.74%	13
62	Intellectual property creation and tech transfer	1.79%	3
63	job placement	0.00%	0
64	law enforcement / policing / security & surveillance	7.14%	12
65	marketing / advertising / promotional activities / outreach / surveys	1.19%	2
66	newly-minted "adults" who don't know what is acceptable yet	1.79%	3
67	pandemic-related (contact tracing, activities, screening)	1.79%	3
68	public square concept (campuses are public spaces…)	0.00%	0
69	research and development, including international	2.38%	4
70	Selling products and services to students	0.00%	0
71	social media	0.60%	1
72	student administration (academics, analytics, grading, class lists, surveys, attendance, registration, discipline)	7.74%	13
73	vendor management	8.33%	14
	Total	100%	168

Q5 - Out of the choices below, please select seven (7) privacy laws / requirements that you believe are most important for universities to follow or most relevant to my study.

#	Answer	%	Count
4	biometric laws / requirements	5.36%	9
7	breach notification or reporting laws / requirements	8.93%	15
8	Can-spam	0.00%	0
9	CCPA (California Consumer Privacy Act)	2.98%	5
10	CMIA (California Medical Information Act - or other similar state law)	1.79%	3
11	The Common rule (US federal research requirements)	2.38%	4
12	consumer protection laws / requirements	3.57%	6
13	COPPA (Children's Online Privacy Protection Act)	1.79%	3
14	data minimization laws / requirements	3.57%	6
15	data retention laws / requirements	5.95%	10
16	data transfer laws / requirements	2.38%	4
17	FCRA (Fair Credit Reporting Act)	0.60%	1
18	FERPA (Family Educational Rights and Privacy Act)	11.31%	19
19	finance laws / requirements	1.19%	2
20	US Federal Trade Commission requirements	2.38%	4
21	GDPR (EU General Data Protection Regulation)	5.36%	9
22	GLBA (US Gramm-Leach-Bliley Act)	1.19%	2
23	health and related laws / requirements	4.17%	7
24	HIPAA (Health Insurance Portability and Accountability Act)	8.93%	15
25	international laws / requirements	2.98%	5
26	IP related laws / requirements	0.00%	0

27	limiting sharing / access laws / requirements	4.17%	7
28	PCI-DSS	2.38%	4
29	policing laws / requirements	1.79%	3
30	security laws / requirements	3.57%	6
31	state privacy laws	7.74%	13
32	website privacy laws and notice requirements	3.57%	6
	Total	100%	168

Q6 - Of the following programmatic elements or activities, please select seven (7) that you feel must be present in a university privacy program.

#	Answer	%	Count
4	automated decision-making insight and processes	1.79%	3
7	board reporting	2.98%	5
8	central oversight	5.36%	9
9	complaint management	2.38%	4
10	consent processes	2.98%	5
11	contract management	0.60%	1
12	CPO / privacy lead designated	8.33%	14
13	culture	1.19%	2
14	data classification and handling matrix	4.17%	7
15	data inventories	4.17%	7
16	data retention	2.98%	5
17	data security policy and program (proactive)	6.55%	11
18	dedicated staff with appropriate resources	4.17%	7
19	department level processes (knowledge of responsibilities, tailored training, participation)	2.38%	4
20	DPIA / PIA (impact assessment) process	3.57%	6
21	DSAR response process and staffing (individual rights)	1.79%	3
22	following a framework / defining model	1.79%	3
23	good recordkeeping and data management	2.38%	4
24	HIPAA assessment	0.60%	1
25	incident response process	3.57%	6
26	insight into research publishing	0.00%	0

27	jurisdictional	0.60%	1
28	leadership / governance	2.38%	4
29	monitoring, audit, assessments	4.76%	8
30	organizational capacity	0.00%	0
31	privacy notices	0.00%	0
32	privacy policies + procedures	6.55%	11
33	privacy program development and implementation	4.76%	8
34	regular reviews of notices and policies	0.60%	1
35	risk register	0.00%	0
36	robust data governance program	1.79%	3
37	security controls	2.98%	5
38	technological elements	0.60%	1
39	third party management (vendors and partners)	5.36%	9
40	training (mandatory, department-specific)	4.17%	7
41	understanding of rights of foreign citizens attending the University	1.79%	3
	Total	100%	168

Q7 - Please select seven (7) risk factors that you feel put universities at risk for noncompliance with privacy laws. What are the critical challenges that universities face in trying to be compliant?

#	Answer	%	Count
4	inadequate funding for data protection programs (privacy / security)	10.71%	18
7	automated admission screenings	0.60%	1
8	data inventories and records of processing are likely nonexistent	2.38%	4
9	decentralized and siloed data systems	8.93%	15
10	departments acting autonomously	2.98%	5
11	employees who don't want to change	1.79%	3
12	existence of sensitive and confidential information in abundance and breadth	7.74%	13
13	extremely diverse activities, data sets, and data subjects	5.95%	10
14	fluctuating population	0.60%	1
15	government run	0.60%	1
16	indefinite retention times for all data	1.79%	3
17	introduction of new technologies	1.79%	3
18	lack of a compliance culture (e.g. faculty and staff who feel they have the autonomy to not follow established policies and procedures)	5.95%	10
19	lack of awareness of laws and policies (and the reasons behind them)	5.36%	9
20	lack of employed or contracted staff that understand privacy	4.17%	7
21	lack of knowledge	1.19%	2
22	lack of overall security and privacy policies through the entire lifecyles	1.79%	3
23	lack of resources generally	2.98%	5
24	lack of resources to focus on record retention, destruction	1.19%	2

25	lack of University Leadership focus & evangelization of Data Privacy as a priority	6.55%	11
26	likelihood or number of individuals with technical skills and likely limited professional maturity not to do something stupid	0.60%	1
27	massive span for data subjects and laws	0.60%	1
28	meaningful informed consent for young adults who may not be sophisticated	0.60%	1
29	misinterpretations that newer privacy laws do not apply	0.00%	0
30	outdated storage requirements	0.00%	0
31	outdated systems	4.76%	8
32	persons ignoring policies	0.60%	1
33	poor data protection controls	4.17%	7
34	research on the cutting edge happens here, the confidentiality of which during creation can make or break future careers	0.00%	0
35	risky activities (like file sharing)	1.19%	2
36	the huge number of sectoral activities at play in the average university	4.17%	7
37	unclear level of responsibilities for various levels of data (i.e., dorm information and access to that information as an example)	2.98%	5
38	universities hold info created about individuals during very formative years of an individual's life	0.60%	1
39	use of health / research data	2.98%	5
41	weak security	1.79%	3
	Total	100%	168

APPENDIX I

ROUND 3 UPVOTED RESPONSES

Privacy in US Universities - Third (Final) Phase

October 11th 2021, 6:51 pm CDT

Q4 - Out of the following 10 top voted activities present at universities or that universities engage in that would trigger privacy laws / standards, please select three (3) that you feel are the most important / most common activities.

#	Question	Total
58	health-related activities (research, student health, workers comp, health centers, occupational reporting, sick leave, insurance claims, reporting)	24
72	student administration (academics, analytics, grading, class lists, surveys, attendance, registration, discipline)	22
61	human capital management / employment (staff / faculty/contractors, applications, management, benefits, salary, contracts / contractors, performance reviews, student reviews, publications)	9
73	vendor management	9
15	data (analytics, capture, control, processing, retention)	8
8	admissions (domestic and foreign)	7
20	finance (billing, payment cards, collections, loans)	5
4	activities and events (marketing, presenters, attendees, purchases, administration, online and remote, in-person)	4
14	counseling	4
64	law enforcement / policing / security & surveillance	1

Q5 - Out of the thirteen (13) top voted choices below, please select three (3) privacy laws / requirements that you believe are most important for universities to follow or most relevant to my study.

Option	Total
FERPA (Family Educational Rights and Privacy Act)	18
limiting sharing / access laws / requirements	11
state privacy laws	10
health and related laws / requirements	10
breach notification or reporting laws / requirements	8
security laws / requirements	7
GDPR (EU General Data Protection Regulation)	7
HIPAA (Health Insurance Portability and Accountability Act)	4
data retention laws / requirements	4
website privacy laws and notice requirements	4
data minimization laws / requirements	4
biometric laws / requirements	2
consumer protection laws / requirements	1

Q6 - Of the following 10 top voted programmatic elements or activities, please select three (3) that you feel must be present in a university privacy program.

Question	Total
privacy program development and implementation	16
CPO / privacy lead designated	15
third party management (vendors and partners)	11
data security policy and program (proactive)	10
dedicated staff with appropriate resources	8
training (mandatory, department-specific)	8
central oversight	6
privacy policies + procedures	6
incident response process	4
monitoring, audit, assessments	3

Q7 - Please select three (3) risk factors that you feel most put universities at risk for noncompliance with privacy laws out of the following eleven (11) top voted factors. What are the critical challenges that universities face in trying to be compliant? The first would be most important, the last would be least important.

Question	Total
decentralized and siloed data systems	17
inadequate funding for data protection programs (privacy / security)	14
existence of sensitive and confidential information in abundance and breadth	11
lack of University Leadership focus & evangelization of Data Privacy as a priority	11
lack of a compliance culture (e.g. faculty and staff who feel they have the autonomy to not follow established policies and procedures)	11
lack of awareness of laws and policies (and the reasons behind them)	7
extremely diverse activities, data sets, and data subjects	6
lack of employed or contracted staff that understand privacy	3
poor data protection controls	3
the huge number of sectoral activities at play in the average university	3
outdated systems	1

Q15 - Is there anything you would like to add about managing privacy at US universities?

If so, please do so below.

1. The problem with privacy at universities is there is so much data in outdated systems, lost repositories, privacy programs in siloes who grew organically with no centralization and now, there are a whole lot of drill sergeants but no general.
2. Universities of course must follow FERPA, so i did not select it. Privacy programs, otherwise, are the same as any other company. Perhaps worse because universities aren't managed like a company, with clear responsibilities, central oversight, and corporate social responsibility goals.
3. it was really difficult to select on three in each category because the complexity of privacy laws applied to the wide range of activities at universities is enormous. My recommendation would be to have centralized management of privacy-focus areas, e.g., hospitals, research, student records, personnel - and treat them like departments reporting up to a chancellor. There needs to be one person who has visibility across the whole system, and it cannot be the CISO. Privacy laws need someone who understand that security is one part of data governance.

REFERENCES

Allen, Peter, Steve Maguire, and Bill McKelvey, eds. 2011. *The SAGE Handbook of Complexity and Management*. London: SAGE.

Amazon.com, Inc. 2021. "Form 10-Q, Period Ending June 30, 2021." U.S. Securities and Exchange Commission. https://d18rn0p25nwr6d.cloudfront.net/CIK-0001018724/cbae1abf-eddb-4451-9186-6753b02cc4eb.pdf.

Asante, Robert. 2019. "Relationship of Organizational Structures in Higher Education to Risk Management." Ed.D., United States -- Pennsylvania: University of Pennsylvania. https://search.proquest.com/pqdtglobal/docview/2388722792/abstract/82A3CAE1CE2A400APQ/11.

Askew, Mike, Valerie Rhodes, Margaret Brown, Dylan Wiliam, and David Johnson. 1997. *Effective Teachers of Numeracy: Final Report*.

Avella, Jay R. 2016. "Delphi Panels: Research Design, Procedures, Advantages, and Challenges." *International Journal of Doctoral Studies* 11: 305–21. https://doi.org/10.28945/3561.

Avuglah, Bright K., Christopher M. Owusu-Ansah, Gloria Tachie-Donkor, and Eugene B. Yeboah. 2021. "Privacy Practices in Academic Libraries in Ghana: Insight into Three Top Universities." *IFLA Journal* 47 (2): 196–208. https://doi.org/10.1177/0340035220966605.

Bach, David, and Abraham L. Newman. 2007. "The European Regulatory State and Global Public Policy: Micro-Institutions, Macro-Influence." *Journal of European Public Policy* 14 (6): 827–46. https://doi.org/10.1080/13501760701497659.

Barrett, Susan M. 2004. "Implementation Studies: Time for a Revival? Personal Reflections on 20 Years of Implementation Studies." *Public Administration* 82 (2): 249–62. https://doi.org/10.1111/j.0033-3298.2004.00393.x.

Bataller-Grau, Juan, Elies Segui-Mas, Javier Vercher-Moll, and Jeffrey W Stempel. 2019. "Constructing More Reliable Law and Policy: The Potential Benefits of the Underused Delphi Method." *Scholarly Works at UNLV Boyd Law* 87 (4): 35.

Bentinck, Salomé A., Clarine J. van Oel, and Machiel J. van Dorst. 2020. "Perception of Privacy in a University Building: The Transparency Paradox." *Frontiers of Architectural Research* 9 (3): 579–87. https://doi.org/10.1016/j.foar.2020.03.004.

Berreby, David. 1996. "Between Chaos and Order: What Complexity Theory Can Teach Business," 8.

Besley, Tina, and Michael A. Peters, eds. 2013. *Re-Imagining the Creative University for the 21st Century*. Creative Education Book Series. Rotterdam: SensePublishers. file:///C:/Users/kroyal/Downloads/[9789462094574%20-%20Re-imagining%20the%20Creative%20University%20for%20the%2021st%20Century]%20The%20Creative%20University_%20Creative%20Social%20Development%20and%20Academic%20Entrepreneurship.pdf.

Bloche, M. Gregg. 2008. "The Emergent Logic of Health Law." *Southern California Law Review* 82: 389.

Bondarouk, Elena, and Ellen Mastenbroek. 2018. "Reconsidering EU Compliance: Implementation Performance in the Field of Environmental Policy." *Environmental Policy and Governance* 28 (1): 15–27. https://doi.org/10.1002/eet.1761.

Borgman, Christine L. 2018. "Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier." https://doi.org/10.15779/Z38B56D489.

Braithwaite, Jeffrey, Kate Churruca, Louise A Ellis, Janet c Long, Robyn Clay-Williams, Nikki Damen, Jessica Herkes, Chiara Pomare, Kristiana Ludlow, and Macquarie University. 2017. *Complexity Science in Healthcare - Aspirations, Approaches, Applications and Accomplishments: A White Paper*.

Broskoske, Stephen L, and Francis A Harvey. 2000. "Challenges Faced by Institutions of Higher Education in Migrating to Distance Learning." Presented at the National Convention of the Association for Educational Communications and Technology, Denver, Colorado, October. https://files.eric.ed.gov/fulltext/ED455761.pdf.

Burdon, Mark, and Paul Telford. 2010. "The Conceptual Basis of Personal Information in Australian Privacy Law," 27.

Burns, Sean. 2020. "The Evolving Landscape of Data Privacy in Higher Education." November 19, 2020. https://library.educause.edu/resources/2020/11/the-evolving-landscape-of-data-privacy-in-higher-education.

Butler, Alan, and Fanny Hidvegi. 2015. "From Snowden to Schrems: How the Surveillance Debate Has Impacted US-EU Relations and the Future of International Data Protection." *Seton Hall Journal of Diplomacy and International Relations* 17: 55.

Bygrave, Lee A. 2008. "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties." SSRN Scholarly Paper ID 915065. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=915065.

Castellacci, Fulvio, Arne Martin Fevolden, and Martin Lundmark. 2014. "How Are Defence Companies Responding to EU Defence and Security Market Liberalization? A

Comparative Study of Norway and Sweden." *Journal of European Public Policy* 21 (8): 1218–35. https://doi.org/10.1080/13501763.2014.916338.

Castells, Manuel. 2000. "Materials for an Exploratory Theory of the Network Society1." *The British Journal of Sociology* 51 (1): 5–24. https://doi.org/10.1111/j.1468-4446.2000.00005.x.

Chunnu-Brayda, Winsome. 2012. "Querying Top-Down, Bottom-Up Implementation Guidelines: Education Policy Implementation in Jamaica." *Journal of Eastern Caribbean Studies* 37 (2): 24–45.

Cohen, Michael. 1999. "Commentary on the *Organization Science* Special Issue on Complexity." *Organization Science* 10 (3): 373–76. https://doi.org/10.1287/orsc.10.3.373.

Computer Hope. 2021. "When Was the First Computer Invented?" March 13, 2021. https://www.computerhope.com/issues/ch000984.htm.

Conceição-Heldt, Eugénia da. 2014. "When Speaking with a Single Voice Isn't Enough: Bargaining Power (a)Symmetry and EU External Effectiveness in Global Trade Governance." *Journal of European Public Policy* 21 (7): 980–95. https://doi.org/10.1080/13501763.2014.912146.

Cropley, A. J. 2001. *Creativity in Education & Learning: A Guide for Teachers and Educators*. Psychology Press.

Cunningham, Roderick. 2004. "An Exploration of the Potential of Complexity Theory for Addressing the Limitations of Current Models of Change and Innovation in Educational Practice.," January, 204.

Detlev, Gabel, and Tim Hickman. 2019. "Chapter 1: Introduction – Unlocking the EU General Data Protection Regulation." White & Case LLP. April 5, 2019. https://www.whitecase.com/publications/article/chapter-1-introduction-unlocking-eu-general-data-protection-regulation.

Diebold, Francis X. 2019. "On the Origin(s) and Development of 'Big Data': The Phenomenon, the Term, and the Discipline." https://www.sas.upenn.edu/~fdiebold/papers/paper112/Diebold_Big_Data.pdf.

Dowding, Martin R. 2011. "Interpreting Privacy on Campus: The Freedom of Information and Personal Privacy and Ontario Universities." *Canadian Journal of Communication* 36 (1): 11–30.

Educause. 2021. “Gramm-Leach-Bliley Act (GLB Act).” Topics: Gramm-Leach-Bliley Act (GLB Act). 2021. https://library.educause.edu/topics/policy-and-law/gramm-leach-bliley-act-glb-act.

El-Khatib, Khalil, Larry Korba, Yuefei Xu, and George Yee. 2003. “Privacy and Security in E-Learning.” *International Journal of Distance Education Technologies (IJDET)* 1 (4): 1–19. https://doi.org/10.4018/jdet.2003100101.

Eppel, Elizabeth. 2017. “Complexity Thinking in Public Administration’s Theories-in-Use.” *Public Management Review* 19 (6): 845–61. https://doi.org/10.1080/14719037.2016.1235721.

Eroğlu, Şahika, and Tolga Çakmak. 2020. “Personal Data Perceptions and Privacy in Turkish Academic Libraries: An Evaluation for Administrations.” *The Journal of Academic Librarianship* 46 (6): 102251. https://doi.org/10.1016/j.acalib.2020.102251.

Esposito, Alicia. 2021. “Could Data Privacy Be Retail’s New Competitive Differentiator?” Retail TouchPoints. September 28, 2021. https://retailtouchpoints.com/topics/security/data-security/could-data-privacy-be-retails-new-competitive-differentiator.

Etzioni, Amitai. 1975. *Comparative Analysis of Complex Organizations, Rev. Ed.* Simon and Schuster.

European Data Protection Board. 2018. “Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version Adopted after Public Consultation | European Data Protection Board.” European Data Protection Board: Guidelines, Recommendations, Best Practices. March 2018. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en.

Fazzini, Kate. 2019. “Kigdom of Lies: Unnerving Adventures in the World of Cybercrime.” Macmillan. 2019. https://read.macmillan.com/lp/kingdom-of-lies/.

Fearn, Carolyn, and Kushwanth Koya. 2021. “Post-GDPR Usage of Students’ Big-Data at UK Universities.” Lecture Notes in Computer Science. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-71292-1_15.

Fink, A., J. Kosecoff, M. Chassin, and R. H. Brook. 1984. “Consensus Methods: Characteristics and Guidelines for Use.” *American Journal of Public Health* 74 (9): 979–83. https://doi.org/10.2105/ajph.74.9.979.

Foden-Vencil, Kristian. 2015. “College Rape Case Shows A Key Limit To Medical Privacy Law.” Jefferson Public Radio. March 10, 2015. https://www.ijpr.org/2015-03-10/college-rape-case-shows-a-key-limit-to-medical-privacy-law.

Fourie, Andria Naude. 2015. “Expounding the Place of Legal Doctrinal Methods in Legal-Interdisciplinary Research.” *Erasmus Law Review* 8 (3): 95–110.

Fullan, Michael. 2001. *Leading in a Culture of Change*. 1st ed. San Francisco: Jossey-Bass.

Gear, Claire, Elizabeth Eppel, and Jane Koziol-Mclain. 2018. “Advancing Complexity Theory as a Qualitative Research Methodology.” *International Journal of Qualitative Methods* 17 (1): 1609406918782557. https://doi.org/10.1177/1609406918782557.

Green, Kenneth C. 2019. “Campus Computing 2019: The 30th National Survey of Computing and Information Technology in American Higher Education.” https://static1.squarespace.com/static/5757372f8a65e295305044dc/t/5da60e02c69e0005bf93690e/1571163656824/Campus+Computing+-+2019+Report.pdf.

Greenley-Giudici, Annie. 2020. “New TrustArc Survey Data Shows Nearly One-Third of Organizations Are Just Starting CCPA Planning | TrustArc.” June 17, 2020. https://trustarc.com/blog/2020/06/17/new-trustarc-survey-data-shows-nearly-one-third-of-organizations-are-just-starting-ccpa-planning/, https://trustarc.com/blog/2020/06/17/new-trustarc-survey-data-shows-nearly-one-third-of-organizations-are-just-starting-ccpa-planning/.

Grobman, Gary M. 2005. “Complexity Theory: A New Way to Look at Organizational Change.” *Public Administration Quarterly* 29 (3/4): 350–82.

Grunig, James E, and Larissa A Grunig. 2001. “Guidelines for Formative and Evaluative Research in Public Affairs,” March, 41.

Gupta, Babita, and Anitha Chennamaneni. 2018. “Understanding Online Privacy Protection Behavior of the Older Adults: An Empirical Investigation.” *Journal of Information Technology Management* XXIX (3): 13.

Gupta, Chetan. 2017. “The Market’s Law of Privacy: Case Studies in Privacy/Security Adoption.” *Washington and Lee Law Review Online* 73 (2): 756.

Gupta, Sunil. 2018. *Driving Digital Strategy: A Guide to Reimagining Your Business*. Harvard Business Review Press.

Hadzieva, Elena, Maja Videnovik, Natasa Koceska, and Vladimir Trajkovik. 2017. “Higher Education from a Complexity Theory Perspective.” In *The Education at the Crossroads - Conditions, Challenges, Solutions, and Perspective*. Bitola. Republic of Macedonia.

Hartman, Francis T., and Andrew Baldwin. 1995. “Using Technology to Improve Delphi Method.” *Journal of Computing in Civil Engineering* 9 (4): 244–49. https://doi.org/10.1061/(ASCE)0887-3801(1995)9:4(244).

Hazy, James, and Murat Erogul. 2021. “A Social Complexity Organization Theory of Collective Leadership.” In *Implementing Complexity Leadership in Practice*. Virtual. https://doi.org/10.5465/AMBPP.2021.12307abstract.

Health Information & the Law Project. 2021. “States | Health Information & the Law.” 2021. http://www.healthinfolaw.org/state.

Hofman, Darra. 2020. “Between Knowing and Not Knowing: Privacy, Transparency, and Digital Records.” Ph.D., University of British Columbia.

Holz, Byron. 2006. “Chaos Worth Having:” *Minnesota Journal of Law, Science, and Technology* 8 (1): 41.

Hornstein, Donald T. 2004. “Complexity Theory, Adaptation, and Administrative Law.” *Duke Law Journal* 54 (4): 913–60.

Hutchinson, Terry, and Nigel Duncan. 2012. “Defining and Describing What We Do: Doctrinal Legal Research.” *Deakin Law Review* 17 (1): 83–119. https://doi.org/10.21153/dlr2012vol17no1art70.

International Association of Privacy Professionals. 2021. “State_Comp_Privacy_Law_Chart.Pdf.” 16 2021. https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.

“Israel: Protection of Privacy Law 5741-1981 (Official Translation).” 1981. Israel.

Jacobson, Michael J., James A. Levin, and Manu Kapur. 2019. “Education as a Complex System: Conceptual and Methodological Implications.” *Educational Researcher* 48 (2): 112–19. https://doi.org/10.3102/0013189X19826958.

Jacoby, Wade, and Sophie Meunier. 2010. “Europe and the Management of Globalization.” *Journal of European Public Policy* 17 (3): 299–317. https://doi.org/10.1080/13501761003662107.

Jerman-Blažič, Borka, and Tomaž Klobučar. 2005. “Privacy Provision in E-Learning Standardized Systems: Status and Improvements.” *Computer Standards & Interfaces* 27 (6): 561–78.

Jones, Gregory Todd. 2007. “Dynamical Jurisprudence: Law as a Complex System.” *Georgia State University Law Review* 24 (4): 873–84.

Jones, Meg Leta, and Lucas Regner. 2016. “Users or Students? Privacy in University MOOCS.” *Science and Engineering Ethics* 22 (5): 1473–96. https://doi.org/10.1007/s11948-015-9692-7.

Kades, Eric. 1996. “The Laws of Complexity and the Complexity of Laws: The Implications of Computational Complexity Theory for the Law.” *Rutgers Law Review* 49 (2): 403–84.

Kerry, Cameron F. 2018. “Why Protecting Privacy Is a Losing Game Today—and How to Change the Game.” *Brookings* (blog). July 12, 2018. https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

Keshavarz, Nastaran, Don Nutbeam, Louise Rowling, and Freidoon Khavarpour. 2010. “Schools as Social Complex Adaptive Systems: A New Way to Understand the Challenges of Introducing the Health Promoting Schools Concept.” *Social Science & Medicine* 70 (10): 1467–74. https://doi.org/10.1016/j.socscimed.2010.01.034.

Kharel, Amrit. 2018. “Doctrinal Legal Research.” SSRN Scholarly Paper ID 3130525. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.3130525.

Klijn, Erik-Hans. 2008. “Complexity Theory and Public Administration: What’s New?” *Public Management Review* 10 (3): 299–317. https://doi.org/10.1080/14719030802002675.

Krishnamurthy, Vivek. 2020. “A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy.” *American Journal of International Law* 114: 26–30. https://doi.org/10.1017/aju.2019.79.

Lama, Amy de la. 2021. “U.S. Biometric Laws & Pending Legislation Tracker.” Bryan Cave Leighton Paisner. May 12, 2021. https://www.bclplaw.com/en-US/insights/us-biometric-laws-and-pending-legislation-tracker.html.

Langenderfer, Jeff, and Anthony D. Miyazaki. 2009. “Privacy in the Information Economy.” *Journal of Consumer Affairs* 43 (3): 380–88. https://doi.org/10.1111/j.1745-6606.2009.01152.x.

Lichtenstein, Benyamin B., and Donde Ashmos Plowman. 2009. “The Leadership of Emergence: A Complex Systems Leadership Theory of Emergence at Successive Organizational Levels.” *The Leadership Quarterly*, Meso-Modeling of Leadership: Integrating Micro- and Macro-Perspectives of Leadership, 20 (4): 617–30. https://doi.org/10.1016/j.leaqua.2009.04.006.

Lockie, Alex. 2017. “Test for Hackers to Become Mid-Grade Officers in US Army Cyber Command.” July 13, 2017. https://www.businessinsider.com/hidden-easter-egg-us-army-cyber-command-puzzle-2017-7.

Lopez, Nicole. 2019. “The Unavoidable and Expanding Impact of GDPR Compliance on Higher Education.” July 2, 2019. https://blog.identityautomation.com/the-unavoidable-and-expanding-impact-of-gdpr-compliance-on-higher-education.

Louis, Karen Seashore, and Matthew B. Miles. 1991. “Managing Reform: Lessons from Urban High Schools.” *School Effectiveness and School Improvement* 2 (2): 75–96. https://doi.org/10.1080/0924345910020202.

Mailthody, Vikram Sharma, James Wei, Nicholas Chen, Mohammad Behnia, Ruihao Yao, Qihao Wang, Vedant Agrawal, et al. 2021. “Safer Illinois and RokWall: Privacy Preserving University Health Apps for COVID-19.” *ArXiv:2101.07897 [Cs]*, March. http://arxiv.org/abs/2101.07897.

Martin, Jeremy. 2019. “Higher Education as a Complex Adaptive System:” *Case Studies*, Emerging Issues in Mathematics Pathways: Case Studies, Scans of the Field, and Recommendations, , 8.

Mason, Jennifer. 1996. *Qualitative Researching*. Qualitative Researching. Thousand Oaks, CA, US: Sage Publications, Inc.

McGregor, Sue L. T. 2020. “Emerging from the Deep: Complexity, Emergent Pedagogy and Deep Learning.” *Northeast Journal of Complex Systems* 2 (1). https://doi.org/10.22191/nejcs/vol2/iss1/2.

Mechanic, David. 1962. “Sources of Power of Lower Participants in Complex Organizations.” *Administrative Science Quarterly* 7 (3): 349–64. https://doi.org/10.2307/2390947.

Miller, Frank E. Acting Director. U.S Department of Education, Family Policy Compliance Office. 2019. “Letter of Finding Regarding Attorney Client Privilege June 2019,” July 28, 2019. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/LetterofFindingRegardingAttorneyClientPrivilegeJuly2019.pdf.

Mitchell, Michael, Michael Leachman, and K. Masterson. 2017. “A Lost Decade in Higher Education Funding State Cuts Have Driven up Tuition and Reduced Quality.” *Undefined*. https://www.semanticscholar.org/paper/A-Lost-Decade-in-Higher-Education-Funding-State-up-Mitchell-Leachman/964f505432c992ee54596ca66316c17cda7e49c6.

Mitleton-Kelly, Eve. 2003. “Ten Principles of Complexity and Enabling Infrastructures.” In *Complex Systems and Evolutioary Perspectives on Organisations: The Application of Complexity Theory to Organisation*. Chapter 2. https://www.researchgate.net/publication/38959109_Ten_principles_of_complexity_and_enabling_infrastructures.

Morçöl, Göktug˘, and Nadezda P. Ivanova. 2010. “Methods Taught in Public Policy Programs: Are Quantitative Methods Still Prevalent?” *Journal of Public Affairs Education* 16 (2): 255–77. https://doi.org/10.1080/15236803.2010.12001596.

Morrison, Keith. 2002. *School Leadership and Complexity Theory*. *Http://Lst-Iiep.Iiep-Unesco.Org/Cgi-Bin/Wwwi32.Exe/[In=epidoc1.in]/?T2000=016224/(100)*. https://doi.org/10.4324/9780203603512.

National Telecommunications and Information Administration. 2018. "Comments of the Alliance of Automobile Manufacturers on the Administration's Approach to Consumer Privacy Submitted in Response to Request for Comments on 'Developing the Administration's Approach to Consumer Privacy' Pursuant to 83 FR 48600, Docket Number 180821780-8780-01." https://www.ntia.doc.gov/files/ntia/publications/aam_privacy_comments.pdf.

Nehf, James P. 2007. "Shopping for Privacy on the Internet." *Journal of Consumer Affairs* 41 (2): 351–75. https://doi.org/10.1111/j.1745-6606.2007.00085.x.

Okoli, Chitu, and Suzanne D. Pawlowski. 2004. "The Delphi Method as a Research Tool: An Example, Design Considerations and Applications." *Information & Management* 42 (1): 15–29. https://doi.org/10.1016/j.im.2003.11.002.

Peruta, Adam, and Alison B. Shields. 2017. "Social Media in Higher Education: Understanding How Colleges and Universities Use Facebook." *Journal of Marketing for Higher Education* 27 (1): 131–43. https://doi.org/10.1080/08841241.2016.1212451.

Petrov, Christo. 2021. "27+ Big Data Statistics - How Big It Actually Is in 2021?" TechJury. October 2, 2021. https://techjury.net/blog/big-data-statistics/.

Pollitt, Christopher. 2009. "Complexity Theory and Evolutionary Public Administration: A Sceptical Afterword." In *Managing Complex Governance Systems*. Routledge.

Rethemeyer, R. Karl, and Natalie C. Helbig. 2005. "By the Numbers: Assessing the Nature of Quantitative Preparation in Public Policy, Public Administration, and Public Affairs Doctoral Education." *Journal of Policy Analysis and Management* 24 (1): 179–91. https://doi.org/10.1002/pam.20079.

Rhodes, Rosamond. 2010. "Rethinking Research Ethics." *The American Journal of Bioethics* 10 (10): 19–36. https://doi.org/10.1080/15265161.2010.519233.

RiskBased Security. 2021. "2020 Year End Report: Data Breach Quickview."

Roman, Jeffrey. 2011. "The Growing Importance of Privacy." June 20, 2011. https://www.bankinfosecurity.com/growing-importance-privacy-a-3761.

Rowe, Gene, and George Wright. 1999. "The Delphi Technique as a Forecasting Tool: Issues and Analysis." *International Journal of Forecasting* 15 (4): 353–75. https://doi.org/10.1016/S0169-2070(99)00018-7.

Royal, K. 2021. "U.S. Quarterly Privacy Update." Webinar, July.

Russell, Carol. 2009. "A Systemic Framework for Managing E-Learning Adoption in Campus Universities: Individual Strategies in Context." *ALT-J* 17 (1): 3–19. https://doi.org/10.1080/09687760802649871.

Saetren, Harald. 2014. "Implementing the Third Generation Research Paradigm in Policy Implementation Research: An Empirical Assessment." *Public Policy and Administration* 29 (2): 84–105. https://doi.org/10.1177/0952076713513487.

Schwartz, Paul M. 2019. "Global Data Privacy: The EU Way." *New York University Law Review* 94 (771): 48.

Schwartz, Paul M., and Karl-Nikolaus Peifer. 2017. "Transatlantic Data Privacy Law." *The Georgetown Law Journal* 106 (1): 115-.

Shey, Heidi. 2014. "Privacy Becomes A Competitive Differentiator In 2015." 2014. https://www.forrester.com/blogs/14-11-12-privacy_becomes_a_competitive_differentiator_in_2015/.

Shey, Heidi, and Enza Iannopollo. 2018. "The State Of Data Security And Privacy: 2018 To 2019." December 5, 2018. https://www.forrester.com/report/The-State-Of-Data-Security-And-Privacy-2018-To-2019/RES137954.

Siemens, George, Shane Dawson, and Kristen Eshleman. 2018. "Complexity: A Leader's Framework for Understanding and Managing Change in Higher Education," 11.

Sisk, Gregory C., and Nicholas Halbur. 2010. "A Ticking Time Bomb - University Data Privacy Policies and Attorney-Client Confidentiality in Law School Settings." *Utah Law Review* 2010 (4): 1277–1314.

Skulmoski, Gregory J., Francis T. Hartman, and Jennifer Krahn. 2007. "The Delphi Method for Graduate Research." *J. Inf. Technol. Educ.* https://doi.org/10.28945/199.

Solove, Daniel J. 2006. "A Brief History of Information Privacy Law," 47.

St. John's University, Information Technology. 2021. "The Gramm-Leach-Bliley Act (GLBA)." The Gramm-Leach-Bliley Act (GLBA). 2021. https://www.stjohns.edu/office-information-technology/technology-labs-and-resources/information-security-and-compliance/gramm-leach-bliley-act-glba.

Sun, Wei, Alisher Tohirovich Dedahanov, Ho Young Shin, and Wei Ping Li. 2021. "Using Extended Complexity Theory to Test SMEs' Adoption of Blockchain-Based Loan System." *PLOS ONE* 16 (2): e0245964. https://doi.org/10.1371/journal.pone.0245964.

Surmiak, Adrianna. 2018. “Confidentiality in Qualitative Research Involving Vulnerable Participants: Researchers’ Perspectives.” *Forum Qualitative Sozialforschung* 19 (September): art.12.

Tarullo, Daniel K. 2004. “The Limits of Institutional Design: Implementing the OECD Anti-Bribery Convention.” *Virginia Journal of International Law* 44 (3): 665-.

Teeter, Derek T. 2017. “Top 5 Common HIPAA ‘Myths’ That Arise in Higher Education.” Husch Blackwell LLP. May 5, 2017. https://www.lexology.com/library/detail.aspx?g=847c698c-493c-4939-b2f4-0ed15f79f69e.

TrustArc. 2021. “So Many States, So Many Privacy Laws.”

Turner, John R., and Rose M. Baker. 2019. “Complexity Theory: An Overview with Potential Applications for the Social Sciences.” *Systems* 7 (4): 23. https://doi.org/doi:10.3390/systems7010004.

United Nations Conference and on Trade and Development. 2020. “Data Protection and Privacy Legislation Worldwide | UNCTAD.” February 4, 2020. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

University of California. 2020. “The Parts of UC.” University of California. December 14, 2020. https://www.universityofcalifornia.edu/uc-system/parts-of-uc.

U.S. Department of Education. 1999. “Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendments (PPRA) Records Systems.” Federal Register. https://www2.ed.gov/notices/sorn/18-05-02_060499.pdf.

U.S. Department of Education, Office of Inspector General. 2018. “Office of the Chief Privacy Officer’s Processing of Family Educational Rights and Privacy Act Complaints.” ED-OIG/A09R0008. https://www2.ed.gov/about/offices/list/oig/auditreports/fy2019/a09r0008.pdf.

U.S. Department of Education, Office of Management. 2018. “Improving the Effectiveness and Efficiency of FERPA Enforcement,” December 20, 2018. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA_Enforcement_Notice_2018.pdf.

U.S. Department of Health and Human Services. 2021. “Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information.” U.S. Department of Health and Human Services, Office for Civil Rights. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

U.S. Federal Trade Commission. 2021. “Statutes Enforced or Administered by the Commission.” Government. Federal Trade Commission. 2021. https://www.ftc.gov/enforcement/statutes.

U.S. News and World Report. 2021. “2022 Best Colleges | College Rankings and Data | US News Education.” 2021. https://www.usnews.com/best-colleges.

Visconti, Cleber. 2018. “(6) Data Privacy: A Competitive Differentiator for the Online Retail Industry | LinkedIn.” January 23, 2018. https://www.linkedin.com/pulse/data-privacy-competitive-differentiator-online-retail-cleber-visconti/.

Wang, Zheng-He, Hai-Lian Yang, Yun-Qing Yang, Dan Liu, Zhi-Hao Li, Xi-Ru Zhang, Yu-Jie Zhang, et al. 2020. “Prevalence of Anxiety and Depression Symptom, and the Demands for Psychological Knowledge and Interventions in College Students during COVID-19 Epidemic: A Large Cross-Sectional Study.” *Journal of Affective Disorders* 275 (October): 188–93. https://doi.org/10.1016/j.jad.2020.06.034.

Warren, Samuel D., and Louis D. Brandeis. 1890. “The Right to Privacy.” *Harvard Law Review* 4 (5): 193–220. https://doi.org/10.2307/1321160.

Wilson, Stephen. 2015. “Big Data Held to Privacy Laws, Too.” *Nature (London)* 519 (7544): 414–414. https://doi.org/10.1038/519414a.

Woods, Chelsea, and Shari Veil. 2020. “Balancing Transparency and Privacy in a University Sexual Misconduct Case: A Legal Public Relations Case Study.” *Journal of International Crisis and Risk Communication Research* 3 (1): 103–36. https://doi.org/10.30658/jicrcr.3.1.5.

Wunderlich, Jens-Uwe. 2012. “The EU an Actor Sui Generis? A Comparison of EU and ASEAN Actorness*.” *JCMS: Journal of Common Market Studies* 50 (4): 653–69. https://doi.org/10.1111/j.1468-5965.2011.02237.x.

Zanfir-Fortuna, Gabriela. 2020. “The General Data Protection Regulation.” *Future of Privacy Forum*, May, 30.

Zhang, Kunbei, and Aernout H. J. Schmidt. 2015. “Thinking of Data Protection Law’s Subject Matter as a Complex Adaptive System: A Heuristic Display.” *Computer Law & Security Review* 31 (2): 201–20. https://doi.org/10.1016/j.clsr.2015.01.007.

Zimmerman, Brenda, Curt Lindberg, and Paul E Plsek. 2013. *Edgeware: Insights from Complexity Science for Health Care Leaders*. United States of America: York University, 1998.

References for Legal Cases

Bowers v. Hardwick, 478 U.S. 186 (1986).

Carpenter v. United States, 585 U.S. ___, 138 S. Ct. 2206 (2018).

Colautti v. Franklin, 439 U.S. 379 (1979).

Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. 2021 EU:C:2020:559. Court of Justice of the European Union.

Doe v. Bolton, 410 U.S. 179 (1973).

Eisenstadt v. Baird, 405 U.S. 438 (1972).

Gonzales v. Carhart, 550 U.S. 124 (2007).

Griswold v. Connecticut, 381 U.S. 479 (1965).

Katz v. United States, 389 U.S. 347 (1967).

Lawrence v. Texas, 539 U.S. 558 (2003).

Mazurek v. Armstrong, 520 U.S. 968 (1997).

Ohio v. Akron Center, 497 U.S. 502 (1990).

Olmstead v. United States, 277 U.S. 438 (1928).

Roe v. Wade, 410 U.S. 113 (1973).

Skinner v. Oklahoma Ex Rel. Williamson, 316 U.S. 535 (1942).

Stanley v. Georgia, 394 U.S. 557 (1969)

Union Pacific Railway Co. v. Botsford, 141 U.S. 250 (1891).

United States v. Vuitch, 402 U.S. 62 (1971).

BIOGRAPHICAL SKETCH

K Royal is an attorney and global privacy professional with over 25 years of experience in the legal and health-related fields. She works with companies from local to global to implement or mature their data governance programs under the increasingly complex network of privacy laws. One of her greatest accomplishments was initiating a program for women in-house attorneys that is now a Global Women in Law and Leadership annual summit by the Association of Corporate Counsel Foundation held at the United Nations in New York. As a multi-racial individual with disabilities and a survivor of domestic violence, she is committed to helping her community, volunteering over 1,000 hours annually. K co-hosts the popular Serious Privacy podcast and has been named an ambassador for the Lupus Foundation of America. K is also a featured technology author for the ACC Docket.

She has received numerous honors for her leadership in both technology and diversity, including Forty-under-40 recipient for Phoenix, named an Outstanding Woman in Business, and Member of the Year for the Association of Corporate Counsel (out 43k members globally). Through each degree (BS, nursing, JD), she has earned honors, including being inducted as a member of the Order of the Barristers (honor society for law school advocacy), Psi Chi (psychology honor society), and Pi Alpha Alpha (public administration honor society).

CURRICULUM VITAE

K ROYAL, JD, FIP, CIPP/US, CIPP/E, CIPM, CDPSE
Tempe, Arizona · kroyal@utdallas.edu

TEACHING AND RESEARCH INTERESTS

As a legal scholar, global data protection professional, lawyer, and former registered nurse, my interests lie at the intersection of technology innovation and global compliance, with a focus on data protection / cyber law and medical / healthcare. As such, I specialize my research and scholarship in emerging technologies, managing change, and combining scholarship with practical application. My current focus has been on my dissertation topic—managing privacy compliance in institutions of higher education taking into account their complexity and broad scope of both activities and data processing. In addition, I am involved with justice, equity, diversity, and inclusivity activities in both service and scholarship, working to address issues such as bias and ethics in AI.

EDUCATION

PhD Candidate, Public Affairs (Defending November 2021)
University of Texas at Dallas
Dissertation topic: Managing Privacy Compliance in U.S. Universities
Juris Doctor, 2004
Sandra Day O'Connor College of Law at ASU
Dual Certificates: IP & Health Law
Associate of Science of Nursing, 1996
University of West Alabama
Bachelor of Science, 1991
Mississippi College
Psychology, with Business Administration

PUBLICATIONS

Journal Articles (and pre-publication presentation)

- Royal, K & Hofman, D. (2012). Impaneled and Ineffective: The Role of Law Schools and Constitutional Literacy Programs in Effective Jury Reform. *Denv. U.L. Rev.*, 90, 959.
- Hofman, D., and Royal, K. "Privacy and Transparency in Their Context: A Problem of Power." 2018 Amsterdam Privacy Conference. October 5 – 8, 2018: Amsterdam, Netherlands.

Practitioner-based Journals

- Royal, K. (2017). Who owns patient medical records? *Journal of Urgent Care Med*., 11(7):21-23.
- Royal, K. (2016). Guns and Urgent Care: How to Respond to Evolving Open-Carry and Concealed-Carry Laws. *Journal of Urgent Care Med*., 10(10):25-29.

- Royal, K. (2015). Protecting Patient Privacy in the Cloud. *Journal of Urgent Care Med*., 10(1):47-49.

Books / Book Chapters

- Chapter author. How the Internet Helps Women with Disabilities. In Carol Smallwood (ed.), Women, Work, and the Web. Chapter 23. December 16, 2014.
- Contributor and reviewer: Canadian Privacy: Data Protection Law and Policy for the Practitioner, 3rd ed. Aron Feuer and Kris Klein (eds). 2018.
- Contributor and reviewer. U. S. Private Sector Privacy, 2d ed. Peter Swire and DeBrae Kennedy-Mayo (eds.). 2018.

Select Industry Articles (and some featured blogs)

- *'My Employer Can't Ask for Proof of Vaccination' and Other Myths Regarding COVID-19 and HIPAA.* Corporate Compliance Insights. September 7, 2021.
- *What You Need to Know About California's New Privacy Rules*. Dark Reading. January 5, 2021.
- *A primer on privacy in Asia-Pacific*. Breitbarth, Moens, and Royal. IAPP. August 25, 2020.
- *Privacy Now: A Dedicated Data Discussion.* ACC Docket. January 1, 2020.
- *Top 5 Legal Tech Trends to Watch in 2020.* ACC Docket. December 2019 (annual feature).
- *Your Vendor, Your Risk*. Maggie Gloeckle and K Royal. ACC Docket. October 1, 2019.
- *How Legal Departments Can Prepare for the Upcoming GDPR*. Law360. March 14, 2018.
- *Cover Your Assets.* Margaret Gloeckle and K Royal. ACC Docket Cover Story September 1, 2017.
- *ePrivacy Regulation: Has Europe Gone Mad?* ACC Docket. June 1, 2017.
- *Finding Equality and Balance in the Face of Legal Typecasting.* K Royal and Tracy Stanton. ACC Docket Cover Story. April 1, 2016.
- *Lawyers: Technological Evolution*. Royal, Nugent, and Reiter. ACC Docket. October 2015.
- *Transferring Personal Data Out of the European Union: Which Export Solution Fits Your Needs?* Katia Bloom and K Royal. ACC Docket. June 1, 2015.
- *Looking at Privacy Law from Trade, Human Rights Perspectives.* IAPP. January 29, 2015.
- *Managing Third-Party Vendors Mitigates Your Risk*, IAPP. 9-part series. 2014- 2015.
- *U.S. Cybersecurity and Medical Devices: Reality Bytes.* K Royal and Gretchen Ramos. ACC Docket. October 2014.
- *Ten Skills that make a Good Privacy Officer.* IAPP. February 19, 2014.
- *The Ethics of Altering Online Profiles During Court Proceedings*. IAPP. September 12, 2013.
- *On Where Health IT and Privacy Meet*. IAPP. September 16, 2013.
- *The Case for a Code*. IAPP. September 1, 2013.
- *What Should You Do If the OCR Sends You a Letter?* IAPP. May 23, 2013.

- *The ABCs of BCRs*. blog entry for the International Association of Privacy Professionals, Privacy Perspectives. May 13, 2013 (generated the highest hits in the blog history).
- *Mail Call: How to Respond to a Regulatory Investigation.* Compliance Today. Health Care Compliance Association. 13(12): 8-11. (December 2011).
- *Genetic Information Nondiscrimination Act of 2008*. Compliance Today. Health Care Compliance Association. 13(3): 45-48. (March 2011).
- *Protecting Patient Data is an All-Inclusive Deal*. Compliance Today. Health Care Compliance Association. 13(1): 44-46. (January 2011).
- *How Much Time? Developing a Medical Records Retention Policy.* Compliance Today. Health Care Compliance Association. 12(9): 8-13. (September 2010).

SELECT HONORS AND AWARDS

- University of Texas at Dallas
  - *Pi Alpha Alpha Honor Society*
- Arizona State University Sandra Day O'Connor College of Law
  - *Matheson Distinguished Service Award (for over 800 hours of pro bono in law school)*
  - *Order of the Barristers*
  - *Pro Bono Highest Distinction*
  - *Maricopa County Outstanding 3L Award*
- University of West Alabama
  - *Outstanding First Year Nursing Student Recipient*
  - *La Société des Quarante Hommes et Huit Chevaux Scholarship*
- Mississippi College
  - *National Merit Scholar*
  - *Psi Chi Honor Society*
- Association of Corporate Counsel, Executive Leadership Council, selected invitation, less than 15 professionals, 2019
- League of Legal Heroes, Sandra Day O'Connor College of Law at Arizona State University, only 15 attorneys selected through peer nomination, November 2018
- Outstanding Women in Business, Phoenix 2017
- Member of the Year, Association of Corporate Counsel, 2015 (> 43k members globally)
- Finalist: Silicon Valley Corporate Counsel Rising Star, 2015
- Presidential Service Award, 2010-2020 (Lifetime Achievement in 2017)
- Selected for FBI Compliance Officers Outreach, 2011 (only 50 nationwide)
- Forty-under-40, Phoenix Business Journal, 2008
- Top 50 Pro Bono Attorney, State Bar of Arizona, 2007
- YWCA Tribute to Women, Education Leader, 2007
- Best Buddies, volunteer and e-buddy since 2004

MEDIA PRESENCE

- Serious Privacy podcast co-host, https://seriousprivacy.buzzsprout.com/
  - Ranked number 1 privacy podcast globally

- James Coker. How 2020 Has Changed the Data Privacy Landscape. infosecurity magazine. December 9, 2020. Quoted.
- Dom Nicastro. What Marketers Need to Know About the California Privacy Rights Act. CMSWire. November 25, 2020. Quoted.
- Joanne Cleaver. GOP Using 'Smart Badges' at Convention, Raising Privacy Flags. Digital Privacy News. August 21, 2020. Quoted.
- Aaron Nicodemus. Without guidance, U.S. companies in limbo after Privacy Shield scrapped, Compliance Week. August 12, 2020. Quoted.
- Stephen Gossett. A Tech Company's Guide to Deleting Personal Identifying Information, Built In (focuses on tech start-ups). June 1, 2020. Quoted.

GLOBAL PROFESSIONAL LEADERSHIP ROLES AND ACTIVITIES

International Association of Privacy Professionals (>65,000 members in 151 countries)

- Active in Leadership Roles (joined in 2009)
    - Research Advisory Board 2019 - 2021
    - Women Leading Privacy Board 2017 - 2019
    - Training Advisory Board 2015 - 2017
    - Publications Advisory Board 2013 – 2015
    - Education Advisory Board 2009 – 2011
- Frequent speaker
- Prolific author
    - Including: developed a vendor management series that was then enlarged to a pre-conference workshop, video training, and special marketing materials

Association of Corporate Council (>43,000 members in in 85 countries)

- Founded a global program for women in-house attorneys (Women in the House)
    - Global Women in Law & Leadership Summit held annually at the United Nations, through ACC Foundation
    - Founding co-chair of the WITH network
- Monthly featured technology and innovation columnist for ACC eDocket
- Health Law Network 2013 – 2017
    - Initiated global pro bono initiative, first for ACC
    - Successive officer roles (engagement, programs, secretary, vice chair, chair)
    - Won network of the year 4 years in a row, causing a win limit to be created
- IT, Privacy, and eCommerce Network 2013 – 2016
    - Initiated ACC's first "in a box" programming
    - Successive officer roles
- Frequent speaker at annual conferences, online programming
- Editorial board, ACC Docket
- Featured technology and privacy columnist
- Annual judge for Thirty-somethings, a recognition program for young professionals

SELECT PRESENTATIONS

Keynote Speaker

- *Multi Jurisdiction Compliance with Data Privacy Laws* (and judge for student poster competition) Governance of Emerging Technologies & Science, 7th Annual Conference. May 2019. Keynote.
- *Success, Diversity, and a cocker spaniel named Lady*. Keynote speaker, University Career Women, ASU, Spring Luncheon, April 2008.

Invited Speaker

- *The Fine Art of Kicking SaaS,* ACC Annual Meeting. October 21, 2021.
- *Privacy Compliance in the Adtech Industry,* ACC Annual Meeting. October 20, 2021.
- *Data management 2021: Cloud, hybrid-cloud and on-prem. How to Manage Complexity, Compliance, and Control,* Data Protection World Forum. July 27, 2021.
- *Microaggressions,* Arizona State Bar CLE. June 11, 2021.
- *Sail into the New HIPAA Safe Harbor.* ePlace Inc., February 23, 2021.
- *All Things California: Updates on the CCPA, Enforcement, and the CPRA,* State Bar of AZ CLE. Presenter. September 2020.
- *Information Blocking.* ePlace Inc., September 24, 2020.
- *New World of Privacy,* FBI Phoenix Citizens Academy Alumni Association. May 2020.
- *POL in IoT: Privacy, Ownership, and Liability. Keynote.* NESST Launch workshop (Network- Embedded, Smart and Safe Things, an industry-university cooperative research center sponsored by the National Science Foundation) May 2019.
- *Privacy Is Not a 4-letter Word: The Relationship Between US and Them–and Emerging Issues*. Institute of Internal Auditors, All Star Conference. October 17-19, 2016.
- *Methods for Protecting Patient Data in the Big Data Revolution*. Invited Speaker and MC. Life Science Data Privacy Conference. July 27, 2015.
- *Privacy and Data Security Risk Management for Health Care Professionals*. Invited speaker. Professional Liability Underwriting Society: 2014 Medical Professional Liability Symposium and 2014 Cyber Liability Symposium. April 24, 2014.

Solo Speaker

- *Update on Global Privacy,* State Bar of Arizona CLE. March 9, 2021.
- *HIPAA Compliance and Best Practices for Records Management.* Webinar. Urgent Care Association of America. June 2010.
- *Privacy Is Not a 4-letter Word: The Relationship Between US and Them–and Emerging Issues*. IIA/ISACA Governance, Risk, and Control Conference. August 17–19 2015.
- *Implementing a Global Whistleblowing Program*. QuickHit Webinar, Health Law Committee, Association of Corporate Counsel. July 1, 2014.
- *Preparing and Updating Your Business Associate Agreement.* Webinar. ePlaceSolutions. May 2011.

Panelist

- *Privacy in the Four Corners of the World and Paper: Managing Privacy Contracts,* Privacy+Security Forum, Fall Academy. September 30, 2021.
- *The Intersection of Healthcare Data & Privacy: How to Navigate the New Challenges,* TrustArc webinar. Organizer and speaker. June 16, 2021.
- *So Many States, So Many Privacy Laws,* TrustArc. Organizer and moderator. April 14, 2021.
- *A New Era of Privacy: Perspectives from Privacy Practitioners,* TrustArc Virtual Summit. Organizer and moderator. March 10, 2021.
- *Privacy 2.0,* TrustArc Virtual Summit. Organizer and moderator. March 10, 2021.
- *Practical Tools for Law Firm Data Security, Privacy, and Cyber Liability,* State Bar of AZ CLE. March 2021.
- *Vendor Management Workshop,* Organizer and Panelist, International Privacy+Security Forum. Organizer and panelist. October 2020
- *How to Leverage GDPR Compliance for CCPA,* TrustArc Webinar. Organizer and moderator. August 2020.
- *The Expanding Universe of Biometric Data: Embrace, Curtail, or Regulate,* Privacy+Security Forum. May 2020.
- *Vendor Management Workshop,* Organizer and Panelist, Privacy+Security Forum. Organizer and panelist. May 2020.
- *What To Expect Next: Planning Goals, AI, and Big Data.* ABA Smart Cities Conference. Feb 2019.
- *GDPR – 1 year later.* SCCE/HCCA Board and Audit Committee Compliance Conference. Feb 2019.
- *To BAA or not to BAA: Understanding and Navigating the Business Associate Agreement*. Organizer and moderator / speaker. Association of Corporate Counsel, Annual Meeting. October 19, 2015.
- *A View from the Hot Seat: Data Breaches and What to Do Now to Make it Easier When it Happens to You.* Association of Corporate Counsel Annual Meeting. October 18–21, 2015.
- *Managing Emerging Technology* (pre-conference workshop). Organizer, moderator, and speaker. IAPP and the Cloud Security Alliance: Privacy, Security, and Risk Conference. September 29–Oct 2, 2015.
- *How to Rock Your Global Privacy Program*. IAPP and the Cloud Security Alliance: Privacy, Security, and Risk Conference. September 29–Oct 2, 2015.
- *Executive Women in Privacy.* Privacy+Security Conference. Washington D.C. October 22, 2015.
- *The Perils of Connectivity: Privacy and Security on the Internet of Things*. State Bar of Arizona Annual Meeting. June 25, 2015.
- *Data Privacy, Information Security Challenges and Cross-border Transfers of Data.* Association of Corporate Counsel. 2015 Corporate Counsel University. May 17-19, 2015.

- *The Future of Cross-Border Mechanism.* International Association of Privacy Professionals. Global Privacy Summit. March 5, 2015.
- *Healthcare Privacy: Diagnosis vs. Prognosis of Hot-button Topics in Healthcare.* International Association of Privacy Professionals. Global Privacy Summit. Preconference workshop. March 4, 2015.
- *Vendor Management Best Practices: The Role of Governance, Risk and Compliance in Vendor Management.* Webinar. TRUSTe Privacy Insight Series. February 19, 2015.
- *Latest in Healthcare Privacy and Security*. Association of Corporate Counsel. Annual Meeting. October 2014.
- *Binding Corporate Rules and Cross-Border Data Transfers*. Association of Corporate Counsel. Annual Meeting. October 2014.
- *Privacy and Data Security Risk Management for Health Care Professionals*. Prof. Liability Underwriting Society: Medical Prof. Liability Symposium and Cyber Liability Symposium. April 24, 2014.
- *Smart Phones, Tablets & the Cloud: Prescription for Disaster?* Professional Liability Underwriting Society: Medical Professional Liability Symposium. April 11, 2013.
- *Impaneled and Ineffective: The Role of Law Schools and Constitutional Literacy Programs in Effective Jury Reform* with Darra Hofman, *Denver Univ. L. Rev.* Vol. 90:4 (October 2013): 959 presented at the 20th Annual Rothgerber Conference, "Public Constitutional Literacy" November 29-30, 2012.
- *To Notify or Not to Notify: that is THE Question*. Professional Liability Underwriting Society: International Conference. November 2010.
- *Cyber Liability: Good Practices. Panelist*. BCS Insurance Conference (Blue Cross). September 2010.
- *Data Breach: Red Flag Rule, HITECH Act, and Litigation Update*. Professional Liability Underwriters Society: 2010 Professional Risk Symposium. March 2010.
- *Innovative Partnerships in law school pro bono*. ABA Equal Justice Works, Law School Preconference, May 2008.

TEACHING EXPERIENCE

Sandra Day O'Connor College of Law at Arizona State University

- Faculty Associate (Adjunct Professor), various courses, online, in-person, and hybrid
    - Privacy, Big Data, & Emerging Technologies (annual Spring course)
    - U.S. Law and Legal Analysis (online 2015 – 2019)
    - Contract Law (2017)
    - *Current course in development: Fundamentals of Privacy Law*

Guest Lecturer

- Laws in the Workplace: a focus on Privacy. Guest lecturer, Human Resources course, University of Texas at Dallas. March 23, 2012.
- Legal Considerations in Health Care. Guest lecturer, Nursing Studies, Arizona State University. Spring 2008.

- Law and Art. Guest lecturer, Interdisciplinary Studies, Arizona State University. Fall 2007, Spring 2008.

OTHER ACADEMIC EXPERIENCE

Sandra Day O'Connor College of Law, Arizona State University (2004 – present)

- Center for Law, Science, and Innovation (LSI)
  - LSI Executive Council (2016 – present)
  - Faculty Fellow, Center for Law, Science and Innovation (2015 – present)
  - Research Fellow, Center for Law, Science, and Innovation (2004 – present)
  - Student cohort leader with other faculty
- Director, Pro Bono and Student Life (2004 – 2008) – Full-time Executive Staff
  - Developed and/or managed local and national volunteer and pipeline programs
  - Several recognized nationally
  - Led student volunteer activities and community partnerships
  - Developed cross-functional activities with other schools and institutions
  - Assisted in developing and implementing two new degree programs
    Managed these degree programs from admissions to graduation
  - Created and managed seminars, symposiums, CLEs, competitions, and speaker series

Barrett, The Honors College at Arizona State University

- Supervisor, Honors Thesis, S.H., 2019 – 2020
- Committee member, Honors Thesis for three students (2018, 2020, 2021)

Community Partnerships in Education

- Developed the Marshall Brennan Constitutional Advocacy Program in Arizona.
  - South Mountain High School in Phoenix
  - Law students taught Constitutional Law to juniors / seniors in collaboration with government and history teachers
  - Included coordination with Law Magnet Program for competitions
- Partnered with the Arizona Foundation for Legal Services and Education to develop a pipeline program from community colleges to law school.
  - Maricopa County Community Colleges
- Partnered with the Hispanic National Bar Association, Sandra Day O'Connor College of Law (led by Prof. Charles Calleros), Los Abogados, the Chicano/Latino Law Students Association, and Phoenix area schools to develop the elementary school to senior attorney MentoRING program.
  - Won numerous awards, including...
  - Adopted by HNBA as national program
  - Calleros, Charles. 2008. Enhancing the Pipeline of Diverse K-12 and College Students to Law School: The HNBA Multi-Tier Mentoring Program. Journal of Legal Education. 58(3): 327 – 340. Available at https://apps.law.asu.edu/files/Current_Students/Student_Life/Pro_Bono_Program/Journal%20Version.pdf

- Further featured in book: Calleros, Charles. 2012: *The Education to the Professions: Programs that Work to Increase Diversity*. Publisher: Location.

Presentations to Student Groups (invited by students, sample list)

- Data Privacy and AI. Law and Science Student Association at Arizona State University in collaboration with Georgetown Cyberlaw. March 3, 2021.
- Women in Technology. Intellectual Property Student Association at Arizona State University. November 19, 2019.
- Exploring Privacy as a Career. Law and Science Student Association at Arizona State University. September 25, 2018.

PROFESSIONAL EXPERIENCE

GLOBAL HEAD OF LEGAL AND PRIVACY
TrustArc (2016 –)

- Associate General Counsel, Data Protection Officer, HIPAA Privacy & Security Officer
- Global scope: e.g., GDPR, PIPEDA, POPIA, LGPD, PIPL
- Multi-industry experience: health care, medical devices, emerging tech, mobile, financial
- Collaborate or lead engagements with government, policy, and industry groups
- Thought leadership, e.g. webinars, guides, templates, blogs, podcast

VICE-PRESIDENT, ASSISTANT GENERAL COUNSEL
CellTrust Corporation (mobile communication) (2015 – 2016)

- Oversaw global compliance and privacy; Privacy officer

PRIVACY COUNSEL
Align Technology, Inc. (global medical device) (2012 – 2017)
Consultant (2015 – 2017)

- Inaugural global privacy counsel for high-tech medical device manufacturer
- First to successfully close both processor and controller EU Binding Corporate Rules
- Worked with European data protection authorities to create processor BCRs

COMPLIANCE OFFICER
Apogee Physicians (direct medical care entity) (2011 – 2012)
First full-time compliance officer responsible for privacy, ethics, and regulatory compliance

PRIVACY & SECURITY OFFICER AND AVP, REGULATORY AFFAIRS
Concentra (direct medical care entity) (2008 – 2011)

- One-person office: > 600 locations, plus lab, wellness, environmental, and auto
- Identified and managed compliance risks from every business line and provided assessment, mitigation, monitoring, and reporting; including training programs

DIRECTOR OF PRO BONO PROGRAMS AND STUDENT LIFE
Sandra Day O'Connor College of Law, Arizona State University (2004 – 2008)

- Led student volunteer activities and community partnerships

- Leadership positions in industry groups and participative in cross-functional efforts.

PRIOR PROFESSIONAL EMPLOYMENT
International Market Analyst (Mobile devices, semiconductors) (2000 – 2001)
Registered Nurse (not actively practicing) (1996 - 2004)

INTERESTING ACTIVITIES

- TED MasterClass, Association of Corporate Counsel, *Inside the Mind of an Attorney*. April 2021.
    - https://www.youtube.com/watch?v=9TYKQ7LW3Q8
- Serious Privacy podcast. Co-host. Consistently ranked high for cybersecurity and privacy
    - https://seriousprivacy.buzzsprout.com/
- Lupus Foundation of America, Ambassador
    - Lupus Advocacy meetings - Sen. Mark Kelly and Rep. Greg Stanton, March 2021
    - Top five fundraising team and individual annually since 2016
- United States of America, Mrs. Arizona 2021
- Featured Woman Professional. *The She Shift: How Women are Changing the Business World.* June 18, 2018. Highlights 25 women in business
- FBI Phoenix Citizens Academy, class of 2008
- Inaugural member, Bar Leadership Institute, State Bar of Arizona, 2007

LICENSES AND GLOBAL CERTIFICATIONS

- State Bar of Arizona, licensed attorney in good standing
- Certified Data Privacy Solutions Engineer (CDPSE) ISACA
- Fellow of Information Privacy, International Association of Privacy Professionals (IAPP)
- Certified Information Privacy Professional (CIPP) for Europe and US, IAPP
- Certified Information Privacy Manager (CIPM), IAPP

SERVICE TO THE COMMUNITY/ ONGOING PRO BONO

- Community Legal Services, Board of Directors,
    - Executive Committee, Technology Committee (chair), Finance Committee
- Sandra Day O'Connor College of Law, Alumni, Board of Directors, Chair
- FBI Phoenix Citizens Academy Alumni Association, Board of Directors
    - Executive Committee, Counsel
- Put on the Cape: A Foundation for Hope, Board of Directors,
    - Executive Committee, Counsel
    - CausePlay volunteer
- Presidential Volunteer Service Award, 2008 – 2020, Lifetime Achievement