University of Washington
Privacy Policy Benchmarking Study

Introduction

This study presents a high-level summary of the emerging local, national, and global **privacy legal landscape**, followed by results of a recent **Privacy Policy benchmarking** initiative undertaken by the UW Privacy Office to identify privacy policy best practices and trends within institutions of higher education.

A well-written privacy policy must support and uphold the many privacy obligations of an institution of higher education:

"Colleges and universities have multiple privacy obligations: they must promote an ethical and respectful community and workplace, where academic and intellectual freedom thrives; they must balance security needs with civil and individual liberties, opportunities for using big data analytics, and new technologies, all of which directly affect individuals; they must be good stewards of the troves of personal information they hold, some of it highly sensitive; and finally, they also must comply with numerous and sometime overlapping or inconsistent privacy laws." [i]

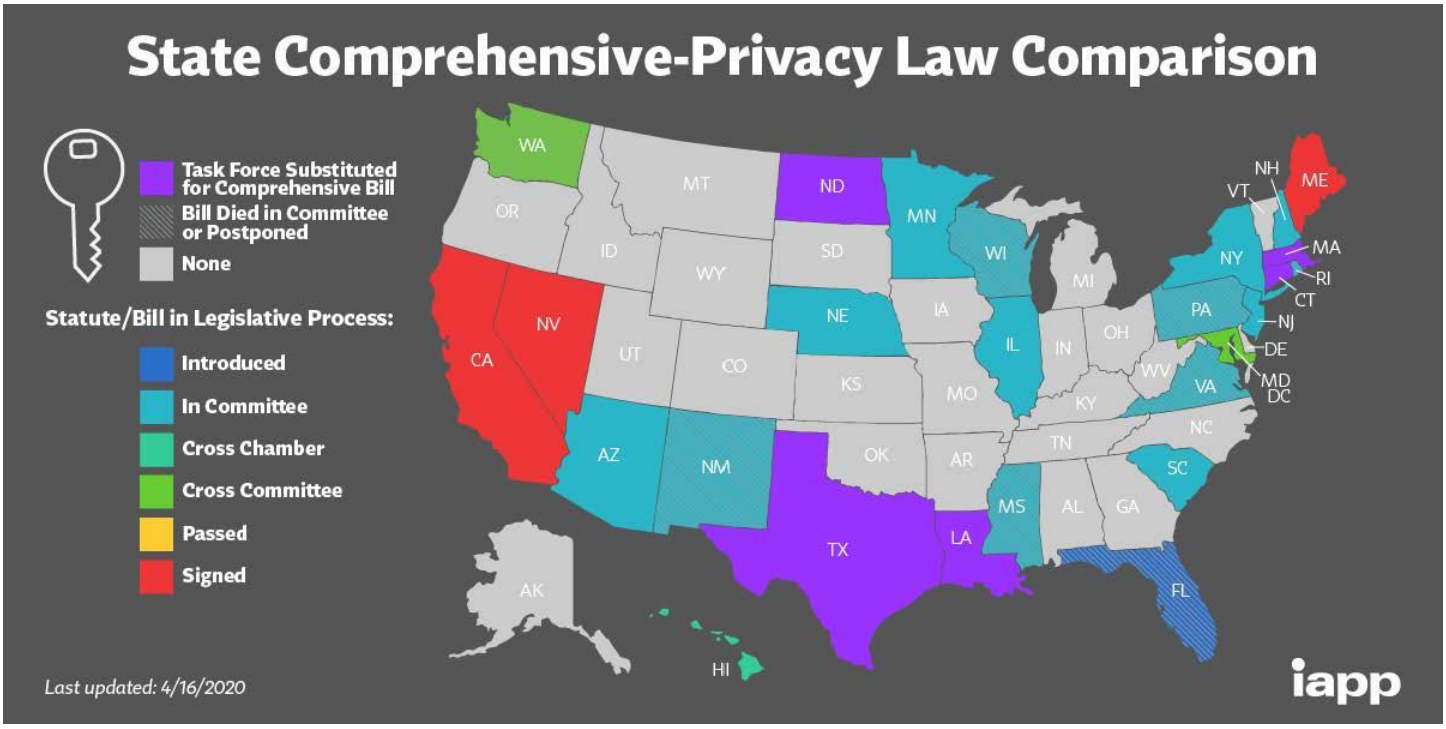
Emerging Privacy Trends in the State of Washington

During the 2020 legislative session, the UW Privacy Office evaluated 14 privacy-related bills introduced or re-introduced in the Washington State legislature, including one which would have enacted a new comprehensive privacy law called the Washington Privacy Act (SSB6281). A similar version of the bill, though highly favored, failed to pass in 2019. While the 2020 Act passed in some form in both the House and Senate, lawmakers were unable to reconcile differences around enforcement authority. Had it passed, the Washington Privacy Act was expected to be viewed as significant privacy legislation, incorporating protections beyond those in the California Consumer Privacy Act (CCPA – one of the most comprehensive consumer privacy laws in the United States). The Washington Privacy Act (taken from Senate Bill Report 2SSB 6281) would have:

- Provided Washington residents with the consumer personal data rights of access, correction, deletion, data portability, and opt out of the processing of personal data for specified purposes.
- Specified the thresholds a business must satisfy for the requirements set forth in this act to apply.
- Identified certain controller responsibilities such as transparency, purpose specification, and data minimization. Required controllers to conduct data protection assessments under certain conditions.
- Provided a regulatory framework for the commercial use of facial recognition services such as testing, training, and disclosure requirements.

Emerging Privacy Trends in the United States

"State-level momentum for comprehensive privacy bills is at an all-time high. After the California Consumer Privacy Act passed in 2018, multiple states proposed similar legislation to protect consumers in their states. The IAPP Westin Research Center compiled the below list of proposed and enacted comprehensive privacy bills from across the country to aid our members' efforts to stay abreast of the changing state-privacy landscape." [ii]



See Appendix A for details about the International Association of Privacy Professionals (IAPP) research efforts to continue evaluation of state legislation using an informative set of consumer rights offered and organizational obligations imposed by such legislation.

Historically at the federal level, the United States has addressed privacy through laws outlining privacy rights and obligations within "silos" of personal information (HIPAA, FERPA, COPPA, PCI-DSS, GLBA, etc.) Recently, multiple comprehensive Privacy Acts have been proposed offering privacy legislation at the federal level (Consumer Online Privacy Rights Act, Consumer Data Privacy Act, bipartisan discussion draft, Consumer Data Privacy and Security Act), though proposed language and provisions have differed widely, and progress on addressing these differences has been slow. In June 2020, the Brookings Institution released a report titled "Bridging the gaps: A path forward to federal privacy legislation," with detailed recommendations about possible strategies to bridge policy gaps and enable federal privacy legislation to proceed. While the COVID-19 pandemic has further raised awareness of the many holes in U.S. privacy law, it has also consumed congressional attention, and the net result may be yet another delay in enacting comprehensive federal privacy legislation, leaving all to cope with the challenges of complying with different privacy provisions in all 50 states. The following quotes effectively capture the challenges of continuing on this path:

"Individual state regulations are no substitute for federal laws, and the inconsistencies from state to state contribute to the "wild west" state of affairs, with different sheriffs in different states drawing different lines in different sands." [iii]

"Among organizations, even those that would prefer this space to remain self-regulated, there is an overwhelming preference for one federal set of rules, rather than 50 different laws from 50 different states." [iv]

Emerging Privacy Trends Globally

Efforts to protect citizens' personal information are expected to accelerate throughout the world as privacy expectations and information technologies continue to evolve. In the 2019 Gartner report entitled "The State of Privacy and Personal Data Protection," one of the strategic assumptions documented captured this trend:

***"Strategic Assumption**: By 2022, half of the planet's population will have its personal information covered under local privacy regulations in line with the General Data Protection Regulation (GDPR), up from one-tenth today."* [v]

That assumption is on its way to becoming a reality, as the Gartner report highlighted the emergence of the following new or revised privacy laws and regulations in just 12 months (from May 2018-May 2019):

Global Privacy Laws enacted: [vi]

- 2018: European Union General Data Protection Regulation (EU GDPR)
- 2018: China's National Standard on Personal Information Protection
- 2018: California Consumer Privacy Act (AB 375)
- 2018: Brazilian General Data Protection Law (LGPD)
- 2019: Japan/EU Adequacy Agreement
- 2019: Thailand Personal Data Protection Act

Gartner isn't the only one making such assumptions. CPO Magazine also noted that *"Laws throughout the world will continue to be updated and implemented, based in part to seek adequacy from the EU. These include Australia, which will look at potentially updating its privacy law, and the Office of the Privacy Commissioner of Canada, which will continue pushing for changes to its privacy law. In addition, India is set to pass its Personal Data Protection law, and other countries will pass or at least consider GDPR-influenced bills on data protection.* [vii]

"In the 12 months from May 2018 to May 2019, privacy regulation has experienced change in all major hubs of data creation, from the U.S. to China and from Europe to Latin America. Many have called it a renaissance, but the fact is that nothing like this has ever happened before." [viii]

Privacy Policy Benchmark Project

The UW Privacy Office conducted a high-level benchmarking project in May-June 2020, intended to assess the current status of privacy policies among other institutions of higher education within the United States.

Initial research was conducted using the following investigative approaches:

1. Locate, review and search within 31+ individual institutional/system websites
2. Review Educause resources compiled within the "Privacy" community group
3. Review International Association of Privacy Professionals resources compiled at iapp.org
4. Review Gartner resources compiled at Gartner
5. Review Educational Advisory Board IT Forum Research Access compiled at Educational Advisory Board (EAB) IT Forum
6. Review and incorporate elements from select, relevant publications

A list of the institutions of higher education explicitly included in this Benchmark effort may be found in Appendix B. When reviewing privacy policies, primary focus was placed on reviewing internally-directed privacy policies rather than reviewing externally-facing privacy notices or statements:

"*External privacy notices and internal privacy policies are two sides of the same coin. One is the commitment to users as to how the organization will handle their personal information and the other provides detailed guidance to employees and partners to deliver on that promise.*" [ix]

Finally, it is important to note that we intentionally omitted from our research content related to incident notification policies or policy elements, handled within UW's Administrative Policy Statement APS 2.5, Information Security and Privacy: Incident Reporting and Management.

Comparative Assessment of Privacy-related Policies

Only one of the higher education institutions reviewed appears to have a comprehensive privacy policy at the institutional level (Penn State). A second institution (University of California, San Diego), has established "Guiding Principles for Personal Data" under their Executive Vice Chancellor – Academic Affairs that "impose" privacy expectations while not in a formal policy. The remainder of colleges and universities address institutional privacy issues across multiple policies, either at the institutional level, or in a subset of organizational policies (e.g. Information Technology Policy). In some institutions, privacy policies are aligned with stakeholder groups: Student Privacy, Employee Privacy, Donor Privacy, etc. Others address privacy by academic or administrative function (Finance, Research, Educational Records), by organizational processes (Privacy in Admissions, Privacy in Healthcare), or (most commonly) by law (FERPA, HIPAA, PCI DSS, EU GDPR, etc.).

The University of California (UC) System has published a set of explicit privacy principles for its system: [x]

- **Autonomy Privacy Principles**:

- Free inquiry
- Respect for individual privacy
- Surveillance ("committed to balancing the need for the safety of individuals and property with the individuals' reasonable expectation of privacy in a particular location.")

- **Information Privacy Principles**:
  - Privacy by Design
  - Transparency and notice
  - Choice
  - Information review and correction
  - Information protection
  - Accountability

In UC San Diego case, this institution has extended "Guiding Principles for Personal Data" to include Data Protection Principles: [xi]

"Personal data must be consistently protected throughout its lifecycle commensurate with its level of sensitivity and criticality to campus operations, regardless of where it resides, type of media, or what purpose it serves. Data collection, retention, use, and sharing practices should be transparent and provide essential protections for the privacy of individuals. When collecting, accessing, using, or disclosing personal data, we commit to the following data protection principles:

- Transparency and individual rights;
- Purpose specification and use limitation;
- Data minimization;
- Access control;
- Security;
- Data quality, accuracy and integrity;
- Due Diligence"

While addressing privacy through multiple policies appear to be the prevailing norm among colleges and universities, there appears to be growing support across professional associations for a single, overarching institutional privacy policy. The Educause "Privacy" community group has had two extensive exchanges about the preference for moving toward a single privacy policy, with benefits well-articulated in this entry:

Having consistent policies across an organization makes it much easier to implement, modify, manage and approve the policies. It also makes it easier to train users, track their acknowledgement of the policies, and get through a regulator's investigation. [xii]

These vast collections of individual policies are clearly necessary, but the key to leadership on ethics and digital ethics is an overarching institutional policy or statement that connects them all. [xiii]

Foundational Elements of a Privacy Policy in Higher Education

Regardless of how privacy-related policies have evolved or how they are structured in higher education, the following is a comprehensive summary of the privacy policy elements typically contained or addressed:

- Purpose of Policy
- Definitions
- Scope
- Roles
- Responsibilities by Role

- Policy Content:
    - Privacy Principles or a link to explicit privacy principles
        - Purposeful handling of personal information
        - Transparency
        - Notice
        - Consent and opt-out
        - Preference Management
        - Data minimization
        - Least privilege access
        - Protection/security
    - Data Classifications/Categories of Information
    - Data retention policies
    - Explicit subject rights (deletion, correction, etc.)
    - Acceptable/Unacceptable tools, practices, and methods (for example, to enable discovery of structured and unstructured personal data, in order to provide the capacity to index and locate personal data, or to identify conditions that justify video surveillance).
    - Risk Assessments and tracking capabilities (including requirements for Privacy Impact Assessments and for Records of Processing Activities when personal information is handled)
    - Link to Privacy Statement/Website Terms & Conditions
    - Other emerging policy/guidance areas (see below)

Emerging Elements of Privacy Policy:

The following content captures high-level emerging privacy policy trends, including level of specificity within policy. These trends have been organized into two categories: privacy rights of individuals, and business expectations and/or obligations to protect privacy. The categories are consistent with IAPP's research paradigm about the state privacy legislative components.

Privacy rights of individuals:

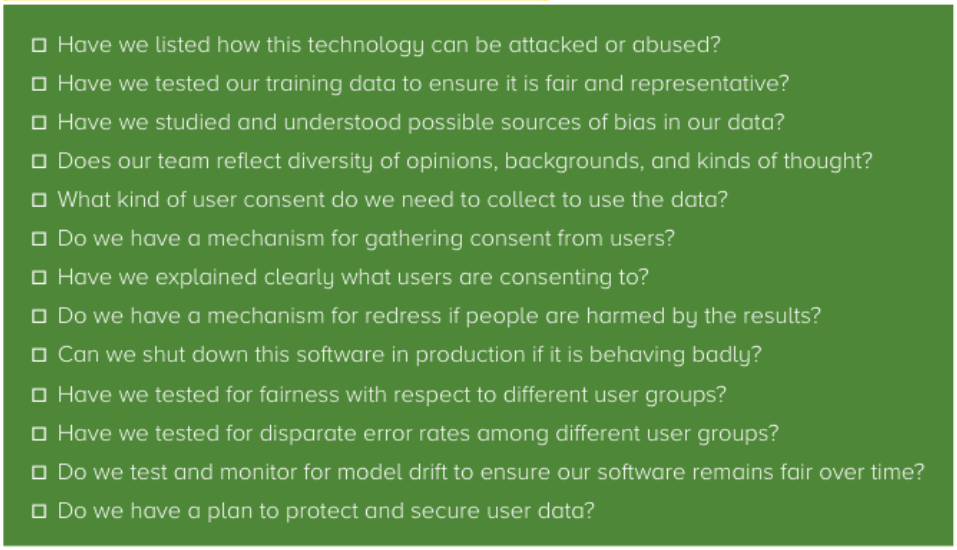
- Differentiating personal data from non-personal data, expanding the definitions of personal data to include biometrics, behaviors, attributes, identification numbers of all types, etc.
- Evolving definitions of sensitive data types, and differential rights/requirements for handling sensitive data, including behavioral data (learning analytics, performance, etc.)

- Privacy notices and options to consent at various levels (by population, by process, etc.)
- Explicit declarations about commitments to privacy ("We do not sell, trade, or rent your personal information to others," or "no expectation of privacy for employees" on internal systems.)

Business obligations to protect privacy:

- Imposing tools to process personal data in encrypted form to minimize risk or to impose data anonymization/pseudonymization
- Requirements for maintenance of data inventories
- Requirements for conducting privacy assessments
- Requirements against proliferating personal information
- Expanded privacy roles (every member of the institution) and more explicit expectations by role
- Institution-wide requirements for annual privacy or confidentiality attestations
- Policies expanded to cover mobile devices, Internet of Things, wearables, etc.
- Explicit lists of approved technologies
- Explicit video surveillance guidance
- Explicit electronic security and access systems guidance
- Explicit guidance about use of data analytics and business intelligence (including artificial intelligence, machine learning, data mining, etc.)
- Guidelines about use of facial recognition (banned in some institutions)
- Guidelines/restrictions regarding use of biometrics
- Explicit cookie policies (including opt out, commitments not to use cookies)
- Explicit online monitoring guidance and limitations
- Inclusion of checklists to ensure privacy by design (example below): [xiv]

Figure 3. Checklist for People Working on Data Projects



Source: DJ Patil, Hilary Mason, and Mike Loukides, "Of Oaths and Checklists," O'Reilly (website), July 17, 2018.

Common Challenges and Pitfalls in Privacy Policy

In reviewing privacy policies and policy elements across various institutions of higher education, the UW Privacy Office observed the following shortcomings:

1. Age of Policy/Guidance: Time since created/last reviewed averaged about approximately 3-5 years. For some, the last date on which the privacy policy was reviewed is over nine years ago. Privacy laws and technologies have shifted significantly since this time, and institutions of higher education do not appear to have privacy policies that are adequately keeping up.
2. Incomplete policy: Vague, lack of explicit elements.
3. Policies related to privacy and data protection have been embedded across multiple policies, which may present a greater challenge in training workforce members and/or in holding them accountable.
4. Inconsistencies across disparate policies, conflicting guidance.
5. Gaps in the holistic approach to privacy of data, vast areas not yet addressed remain invisible to campus.
6. Policy management across disparate policies is time-consuming and can be more expensive (time, lawsuits, fines, sanctions, etc.).

Another daunting reality is the simple fact that at about the time we have fully wrapped our minds around the current set of worries, pitfalls, outrages, and solutions, there will be a new set of digital ethics quandaries before us. [xv]

Conclusion

As global privacy laws shift and expand, institutions of higher education will increasingly be challenged to ensure privacy policies and practices consistent with evolving compliance requirements.

Further, and perhaps even more challenging, will be the institutional need to offer clear, coherent, comprehensive privacy policies (and supporting resources) to successfully address emerging technological advancements as well as evolving citizen expectations around privacy and data ethics. Our stakeholders will look us to be exemplary data stewards as we continue to pursue the teaching, research and service missions of our respective academic institutions.

ENDNOTES:

[i] EDUCAUSE resource: **The Higher Education CPO Primer, Part 1: A Welcome Kit for Chief Privacy Officers in Higher Education**, page 4. August, 2016. From the Higher Education Information Security Council (HEISC) in partnership with EDUCAUSE https://library.educause.edu/-/media/files/library/2016/8/cpoprimerpart1.pdf

[ii] International Association of Privacy Professionals (IAPP) "**US State Comprehensive Privacy Law Comparison,"** Last updated: 4/16/2020. https://iapp.org/resources/article/state-comparison-table/

[iii] John O'Brien, President and CEO of EDUCAUSE, "**Digital Ethics in Higher Education 2020**" EDUCAUSE Review, 2020 Issue #2, Volume 55, Number 2, May 18, 2020. https://er.educause.edu/toc/educause-review-print-edition-volume-55-number-2-2020-issue-2, page 33

[iv] Nader Henein, Bart Willemsen, **"The State of Privacy and Personal Data Protection, 2019-2020,"** Published 15 April 2019, ID G00376084. https://www.gartner.com/doc/3906874, page 4 of 16

[v] Nader Henein, Bart Willemsen, **"The State of Privacy and Personal Data Protection, 2019-2020,"** Published 15 April 2019, ID G00376084. https://www.gartner.com/doc/3906874, page 2 of 16

[vi] Nader Henein, Bart Willemsen, **"The State of Privacy and Personal Data Protection, 2019-2020,"** Published 15 April 2019, ID G00376084. https://www.gartner.com/doc/3906874, page 2 of 16

[vii] Anne Kimbol, **"Emerging Trends: What to Expect From Privacy Laws in 2020,"** CPO Magazine, January 29, 2020. https://www.cpomagazine.com/data-protection/emerging-trends-what-to-expect-from-privacy-laws-in-2020/

[viii] Nader Henein, Bart Willemsen, **"The State of Privacy and Personal Data Protection, 2019-2020,"**Published 15 April 2019, ID G00376084. https://www.gartner.com/doc/3906874, page 3 of 16

[ix] Nader Henein, Bart Willemsen, **"The State of Privacy and Personal Data Protection, 2019-2020,"** Published 15 April 2019, ID G00376084. (Gartner log-in required) https://www.gartner.com/doc/3906874, page 8 of 16

[x] University of California "UC Statement of Privacy Values," pages 2-4. https://www.ucop.edu/ethics-compliance-audit-services/_files/compliance/uc-privacy-principles.pdf

[xi] University of California San Diego Executive Vice Chancellor – Academic Affairs website, **"Guiding Principles for Personal Data,"** https://evc.ucsd.edu/units/privacy/guiding-principles-personal-data.html

[xii] Listserv respondent, from the **Archives of the EDUCAUSE Privacy Community Group listserv** (630 subscribers), email extracted in July 2019. http://listserv.educause.edu/scripts/wa.exe?A0=PRIVACY

[xiii] John O'Brien, President and CEO of EDUCAUSE, "**Digital Ethics in Higher Education 2020**" EDUCAUSE Review, 2020 Issue #2, Volume 55, Number 2, May 18, 2020. https://er.educause.edu/toc/educause-review-print-edition-volume-55-number-2-2020-issue-2, page 38

[xiv] John O'Brien, President and CEO of EDUCAUSE, "**Digital Ethics in Higher Education 2020**" EDUCAUSE Review, 2020 Issue #2, Volume 55, Number 2, May 18, 2020. https://er.educause.edu/toc/educause-review-print-edition-volume-55-number-2-2020-issue-2, page 39

[xv] John O'Brien, President and CEO of EDUCAUSE, "**Digital Ethics in Higher Education 2020**" EDUCAUSE Review, 2020 Issue #2, Volume 55, Number 2, May 18, 2020. https://er.educause.edu/toc/educause-review-print-edition-volume-55-number-2-2020-issue-2, page 42

ADDITIONAL REFERENCES

1. Cameron Kerry, **"Keeping the fires burning for federal privacy legislation,"** IAPP Privacy Perspectives, June 3, 2020. https://iapp.org/news/a/keeping-the-fires-burning-for-federal-privacy-legislation/

2. Ron DeJesus, Founder and CEO DeJesus Consulting, **"How to operationalize privacy by design**," IAPP The Privacy Advisor, May 27, 2020. https://iapp.org/news/a/how-to-operationalize-privacy-by-design/

3. Lisa Ho, Campus Privacy Office at University of California, Berkeley, **"Naked in the Garden: Privacy and the Next Generation Digital Learning Environment,"** EDUCAUSE Review, July 31, 2017. https://er.educause.edu/articles/2017/7/naked-in-the-garden-privacy-and-the-next-generation-digital-learning-environment

4. Nick Jones, David Cearley, **"Gartner Top 10 Strategic Technology Trends for 2020: Transparency and Traceability,"** March 10, 2020, ID G00450644. https://www.gartner.com/doc/3981951

5. Bart Lazar, "**Five Key Provisions a Federal Privacy Law Should Include,"** CPO Magazine, June 1, 2020. https://www.cpomagazine.com/data-protection/five-key-provisions-a-federal-privacy-law-should-include/

6. Emily Leach, Kevin Donahue, **"Embedding data ethics into your 'culture of privacy',"** IAPP The Privacy Advisor, May 27, 2020. https://iapp.org/news/a/embedding-data-ethics-into-your-culture-of-privacy/

7. Bernard Woo, Bart Willemsen, "**Gartner for IT Leaders: Toolkit Privacy Policy,"** September 6, 2019, ID G00432942. https://www.gartner.com/doc/3957023

Appendix A

UNIVERSITY *of* WASHINGTON

PRIVACY OFFICE

IAPP State Table of privacy legislation and rights/obligations

State Comprehensive-Privacy Law Comparison

Bills introduced 2018-2020

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 (s = security only)	Strict Age Opt-in for or Prohibition on Sale of Information	Business Obligations: Notice/Transparency Requirement	Data Breach Notification	Risk Assessments	Prohibition on Discrimination (exercising rights)	Purpose Limitation	Processing Limitation	Fiduciary Duty
Arizona		SB 1614		x		x			x			16				x			
Arizona[I]		HB 2729		x	x	x	x	x	x										
California		**AB 375/SB 1121**	**California Consumer Privacy Act**	**x**		**x**		**x**	**x**		**s**	**16**	**x**			**x**			
Connecticut		RB 1108		Task force substituted for comprehensive bill.															
~~Florida~~		~~H 963~~							~~x~~			~~x~~							
Hawaii[II]		HB 2572							p										
Hawaii		HCR 225		Task force substituted for comprehensive bill.															
~~Hawaii~~		~~SB 418~~		~~x~~		~~x~~		~~x~~	~~x~~			~~16~~	x			~~x~~			
Illinois		SB 2263	Data Privacy Act	x	x	x		x	x				x		x				
Illinois		SB 2330	Illinois Data Transparency and Privacy Act	x	x	x	x	x	x		s		x		x	x			
Illinois		HB 5603	Consumer Privacy Act	x		x		x	x		s	16	x			x			
Louisiana		HR 249		Task force substituted for comprehensive bill.															
Maine[III]		**LD 946[I]**	**An Act to Protect the Privacy of Online Consumer Information**				**x**		**in**				**x**			**x**			
~~Maryland~~		~~HB 249~~							~~x~~							~~x~~			
Maryland[IV]		HB 784	Online Consumer Protection Act	x		x		x	x				x			x			
Maryland[V]		HB 1656		x		x		x	x		s	16	x			x			
Massachusetts		S 120		Study order issued.															
Minnesota		HF 3936	Minnesota Consumer Data Privacy Act	x	x	x		x	x				x		x	x	x	x	
~~Mississippi~~		~~HB 1253~~	~~Mississippi Consumer Privacy Act~~	~~x~~		~~x~~		~~x~~	~~x~~		~~s~~	~~16~~	~~x~~			~~x~~			
Nebraska		LB 746	Nebraska Consumer Data Privacy Act	x		x			x			16	x			x			
Nevada		**SB 220/Ch. 603A**							**x**				**x**	**x**					
New Hampshire[VI]		HB 1236									x								
New Hampshire		HB 1680		x		x		x	x		s		x			x			
New Jersey		A 2188		x					x				x			x			
New Jersey[VII]		A3255		x		x		x	in		x		x			x			
~~New Jersey~~		~~S 2834~~		~~x~~					~~x~~				~~x~~			~~x~~			
~~New Mexico~~		~~SB 176~~	~~Consumer Information Privacy Act~~	~~x~~		~~x~~		~~x~~	~~x~~		~~s~~	~~18~~	~~x~~			~~x~~			
New York		S 224	Right to Know Act					x					x						
New York		S 5642	New York Privacy Act	x	x	x	x	x	x	x	x		x	x				x	x
North Dakota		HB 1485		Task force substituted for comprehensive bill.															
~~Pennsylvania~~		~~HB 1049~~	~~Consumer Data Privacy Act~~	~~x~~		~~x~~			~~x~~		~~s~~	~~16~~	~~x~~			~~x~~			
~~Rhode Island~~		~~S 0234~~	~~Consumer Privacy Protection Act~~	~~x~~		~~x~~		~~x~~	~~x~~		~~x~~	~~16~~	~~x~~			~~x~~			
South Carolina[VIII]		H 4812	South Carolina Biometric Data Privacy Act	x		x			x		x	16	x	x		x	x	x	
Texas		HB 4390	Texas Privacy Protection Act	Task force substituted for comprehensive bill.															
~~Texas~~		~~HB 4518~~	~~Texas Consumer Privacy Act~~	~~x~~		~~x~~		~~x~~	~~x~~			~~16~~	~~x~~			~~x~~			
~~Virginia~~		~~HB 473~~	~~Virginia Privacy Act~~	~~x~~	~~x~~	~~x~~	~~x~~	~~x~~	~~x~~		~~x~~		~~x~~		~~x~~				
~~Washington~~		~~SB 6281~~	~~Washington Privacy Act~~	~~x~~	~~x~~	~~x~~		~~x~~	~~x~~				~~x~~		~~x~~	~~x~~	~~x~~	~~x~~	
~~Wisconsin~~		~~AB 870~~	~~Wisconsin Data Privacy Act (I)~~	~~x~~									~~x~~	~~x~~			~~x~~		
~~Wisconsin~~		~~AB 871~~	~~Wisconsin Data Privacy Act (II)~~			~~x~~													
~~Wisconsin~~		~~AB 872~~	~~Wisconsin Data Privacy Act (III)~~				~~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~~

s - private right of action for security violations only
in - opt-in consent requirement
p - prohibition without consent

[I] Arizona HB 2729's right of deletion only requires deletion if one of five requirements is satisfied (rather than an absolute right with exemptions, it is a conditional right)

[II] Hawaii HB 2572 is the trimmed-down result of the comprhensive recommendations made by the HCR 225 task force; prohibits the sale of geolocation information and internet browser information without consent; updates parameters for government entity access to electronically stored data

[III] Maine LD 946 applies only to internet service providers

[IV] Maryland HB 784 passed the Maryland House, but received an unfavorable report by the Senate Finance Committee; its continued progression is in doubt

[V] Maryland HB 1656 prohibits the knowledgable or wilfully disregarded disclosure of personal information of individuals under age 16 to third parties

[VI] New Hampshire HB 1236 creates a general private right of action for violations of a an individual's expectation of privacy in personal information shared with third-party providers of information and services

[VII] New Jersey A3255 includes a right to opt in for the sale of information and the collection of information

[VIII] South Carolina H 4518 applies only to biometric information

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

iapp

Last updated: 4/16/2020

(List below copied from IAPP website https://iapp.org/resources/article/state-comparison-table/)

The 16 common privacy provisions include the following:

- **The right of access to personal information collected or shared –** The right for a consumer to access from a business/data controller the information or categories of information collected about a consumer, the information or categories of information shared with third parties, or the specific third parties or categories of third parties to which the information was shared; or, some combination of similar information.
- **The right to rectification** — The right for a consumer to request that incorrect or outdated personal information be corrected but not deleted.
- **The right to deletion** — The right for a consumer to request deletion of personal information about the consumer under certain conditions.
- **The right to restriction of processing** — The right for a consumer to restrict a business's ability to process personal information about the consumer.
- **The right to data portability** — The right for a consumer to request personal information about the consumer be disclosed in a common file format.
- **The right to opt out of the sale of personal information** — The right for a consumer to opt out of the sale of personal information about the consumer to third parties.
- **The right against solely automated decision making** — A prohibition against a business making decisions about a consumer based solely on an automated process without human input.
- **A consumer private right of action** — The right for a consumer to seek civil damages from a business for violations of a statute.
- **A strict opt-in for the sale of personal information of a consumer less than a certain age** — A restriction placed on a business to treat consumers under a certain age with an opt-in default for the sale of their personal information.
- **Notice/transparency requirements** — An obligation placed on a business to provide notice to consumers about certain data practices, privacy operations, and/or privacy programs.
- **Data breach notification** — An obligation placed on a business to notify consumers and/or enforcement authorities about a privacy or security breach.
- **Mandated risk assessment** — An obligation placed on a business to conduct formal risk assessments of privacy and/or security projects or procedures.
- **A prohibition on discrimination against a consumer for exercising a right** — A prohibition against a business treating a consumer who exercises a consumer right differently than a consumer who does not exercise a right.
- **A purpose limitation** — An EU General Data Protection Regulation–style restrictive structure that prohibits the collection of personal information except for a specific purpose.
- **A processing limitation** — A GDPR-style restrictive structure that prohibits the processing of personal information except for a specific purpose.
- **Fiduciary duty** — An obligation imposed on a business/controller to exercise the duties of care, loyalty, and confidentiality (or similar) and act in the best interest of the consumer.

Appendix B:

Institutions of Higher Education included in the benchmarking research:

- Carnegie-Mellon University
- Case Western Reserve
- Cornell
- Duke University
- Georgia Tech
- New Mexico State University
- Notre Dame
- Ohio State University
- Penn State University
- Purdue
- Temple University
- Texas A & M
- University of California - System Level
- University of California – Davis
- University of California – Berkeley
- University of California – Los Angeles
- University of California – San Diego
- University of California – Santa Cruz
- University of Colorado
- University of Connecticut
- University of Florida
- University of Illinois - Urbana-Champaign
- University of Kentucky
- University of Manitoba
- University of Miami
- University of Michigan – Ann Arbor
- University of New Mexico
- University of North Carolina – Chapel Hill
- University of Pennsylvania
- University of Texas - system level
- Wayne State University