OFFICE OF

Information Technology Services

Information Security

21st Century Privacy Law Task Force
November 15, 2019

Brook Conner,
Assistant Superintendent, CIO

Bob Strickland,
Director, CISO

Office of Information Technology Services

Exercises technical oversight of information and telecommunication systems, facilities, and services of the public school system and department-wide operations to ensure that information technology and telecommunications support are being provided efficiently and effectively, and in accordance with laws, policies, and accepted principles of management.

Information Security Program

The Hawaii Department of Education's Information Security Program consists of a framework for creating a secure and safe computing environment for our students, teachers, and administrators that allows them to achieve their success. Key elements include:

- Information Security & Privacy
- Risk Management
- Identity and Access Management
- Vulnerability Management & Incident Response
- Security Awareness Training
- IT Investigations

Technology Vision and Roadmap

Solution Life Cycle

Replace

[only break-fix]

- ODS, ADS
- SSES
- LDS
- eCSSS
- SharePoint
- Lotus Notes
- FMS

Modernize

[careful consideration]

- Payroll
- Budget
- eHR
- Time&Attendance

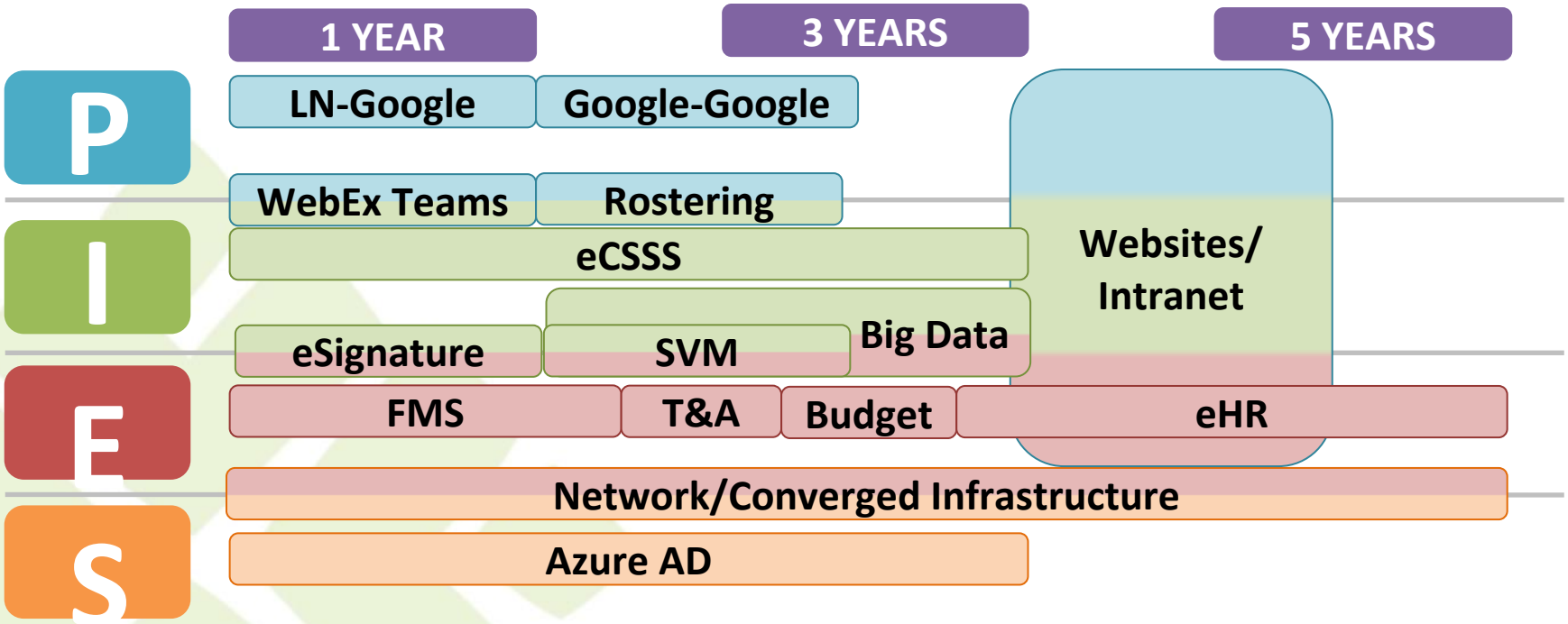
Strategic

[invest]

- Infinite Campus
- Google/Gsuite
- Azure AD
- ServiceNow

Technology Vision and Roadmap

TIMELINE: Replace & Modernize



Student Information System

Infinite Campus

- Cloud based service - manages student data including PII
- Family Educational Rights & Privacy Act (FERPA) compliant - will not redisclose PII without the consent of a parent, guardian, or eligible student
- Employs extensive technological and operational measures to ensure data security and privacy, including advanced security systems technology, physical access controls, and annual privacy training for employees and partners
- Undergoes annual security audits including an external SOC 2 Type II audit
- All data housed within the United States
- Infinite Campus does not own any of the student data

Productivity and Collaboration Software

G Suite for Education

- Cloud based service - hosts documents, spreadsheets, and user data that may include student records and PII
- The data stored in Google G-Suite for Education is encrypted at rest and in transit (within the HIDOE domain)
- Access to storage and files in G Suite is permissions based
- Hawaii Department of Education Administrators have access to powerful security tools provided by Google for domain administration
- ISO 27001 compliant
- FERPA and COPPA Compliant
- Google does not own any student data

Financial Management System

Conducting an RFP to replace the current on-prem FMS system with a cloud based ERP service

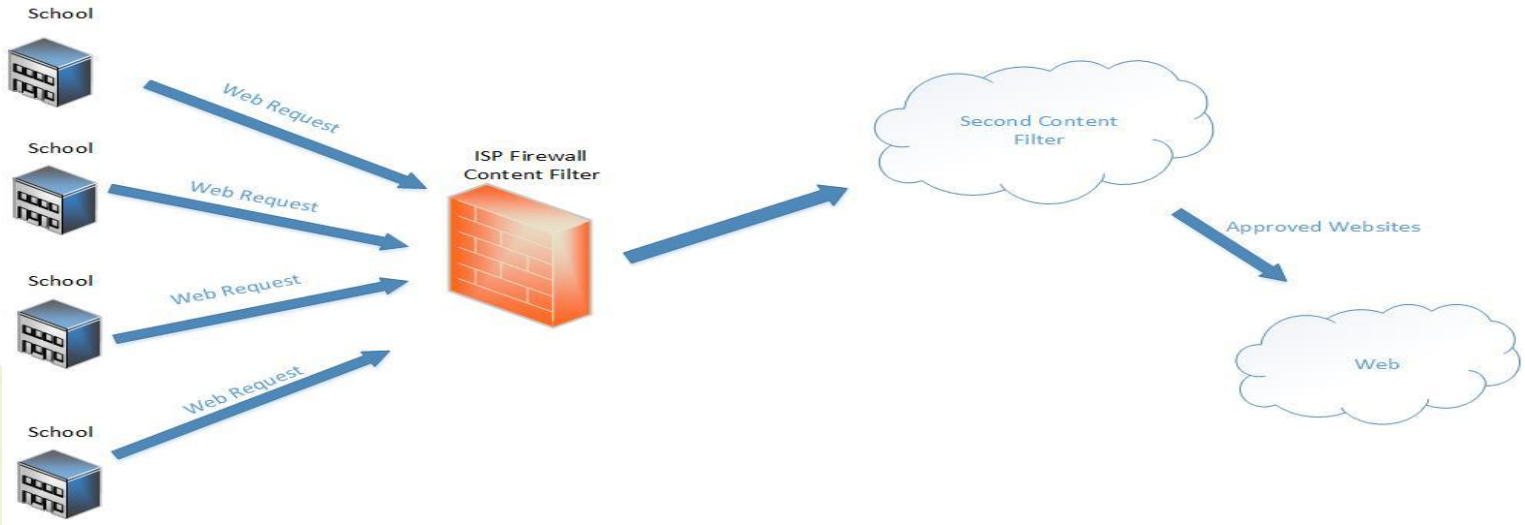
Key areas for security review include:

- Physically secure data centers
- Replication of data across regions to support disaster recovery
- Encryption of data at rest and in transit
- Role Based Access Control (security principle of least privilege)
- Third party penetration testing and security audits
- Security logs for activities related to operating system, applications, databases, and network devices
- Isolation of vendor access to HIDOE financial management data

Data Sharing Agreements with Vendors

- Periodically, vendors request access to student data when engaged in a sponsored project or initiative
- All Data Sharing Agreements are reviewed and approved by the Data Governance organization within the DOE and the Attorney General's Office
- A review of the agreement is conducted by the DOE security team to ensure secure transmission of data and safe storage and access of data by the third party
- All vendors are required to abide by the Hawaii data breach notification law (487 N)
- Future capability includes vendor scoring with GRC/IRM applications

Multiple Layers of Security



- Endpoints - Anti-virus (decentralized)
- Firewall - Content Filtering, Access Control
- Cloud Security Service Provider - Content Filtering, Threat Detection, Blocking of Malicious and inappropriate Domains
- Email - Anti-spam

Anti-Malware Protection (scans and removes malicious software)

October 2019

Category	Detection Count
PUP	136419
Website	12250
Malware	9616
PUM	8192
Exploit	156
Ransomware	1
Grand Total	**166634**

Content Filtering - Inappropriate Websites

Prevented Access to Inappropriate Websites

Identity	Destination	Identity Used by Policy	Internal IP	External IP	Action	Categories	A
HIDOE QLC	pushosubk.com	HIDOE QLC		165.248.216.193	Blocked	**Illegal Downloads**	
HIDOE QLC	dailythemedcrosswordanswers.com	HIDOE QLC		165.248.216.193	Blocked	**Academic Fraud**	
HIDOE QLC	vpn.vonvpn.com	HIDOE QLC		165.248.216.193	Blocked	**Proxy/Anonymizer**	
HIDOE QLC	vpn.vonvpn.com	HIDOE QLC		165.248.216.193	Blocked	**Proxy/Anonymizer**	
HIDOE QLC	www.leafly.com	HIDOE QLC		165.248.216.193	Blocked	**Drugs**	
HIDOE QLC	s3.zerochan.net	HIDOE QLC		165.248.216.193	Blocked	**Lingerie/Bikini,** Anime/Manga/Webcomic	
HIDOE QLC	e42d6d51b521.celestial.mobi	HIDOE QLC		165.248.216.193	Blocked	**Illegal Downloads**	
HIDOE QLC	services.disconnect.me	HIDOE QLC		165.248.216.193	Blocked	**Proxy/Anonymizer, Personal VPN**	
HIDOE QLC	www.meme-arsenal.com	HIDOE QLC		165.248.216.193	Blocked	**Adult Themes,** Humor	
HIDOE QLC	adserver.adreactor.com	HIDOE QLC		165.248.216.193	Blocked	**Adware, Web Spam,** Business Services	
HIDOE QLC	pushosubk.com	HIDOE QLC		165.248.216.193	Blocked	**Illegal Downloads**	
HIDOE QLC	dns.google.com	HIDOE QLC		165.248.216.193	Blocked	**Proxy/Anonymizer,** Search Engines	
HIDOE QLC	services.disconnect.me	HIDOE QLC		165.248.216.193	Blocked	**Proxy/Anonymizer, Personal VPN**	
HIDOE QLC	services.disconnect.me	HIDOE QLC		165.248.216.193	Blocked	**Proxy/Anonymizer, Personal VPN**	
HIDOE QLC	nhentai.net	HIDOE QLC		165.248.216.193	Blocked	**Adult Themes, Nudity, Pornography,** Anime/Manga/Webcomic	

Inbound Mail Filtering (One Month)

Incoming Mail Details

Items Displayed: 10

Sender Domain	Total Attempted	Stopped by Reputation Filtering	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Detected by Advanced Malware Protection	Stopped by Content Filter	Stopped by DMARC	Total Threat	Marketing	Social	Bulk	Total Graymails	Clean
google.com	2.9M	66.5k	16	3,991	1	0	14.2k	0	84.7k	0	0	0	0	2.8M
elabs12.com	190.2k	0	0	0	0	0	0	0	0	0	0	0	0	190.2k
amazonses.com	83.9k	486	0	152	0	0	19	0	657	0	0	0	0	83.3k
outlook.com	74.0k	0	7	0	0	0	124	0	131	0	0	0	0	73.9k
constantcontact.com	46.3k	1,797	0	69	0	0	0	0	1,866	0	0	0	0	44.5k

Information Security Program Coordination

- OITS partners with Complex Area technical support staff in an effort to provide technology services that are supported, safe, and secure
- Schools in many cases have their own technical support teams responsible for endpoint security including OS patching, anti-virus & anti-malware programs
- Information Technology Managers and Technical Coordinators at the schools coordinate security incident response
- Internet content filters and safe search capability ensure Children's Internet Protection Act (CIPA) compliance from the classroom
- Schools create websites but do not host student records including PII

Questions/Suggestions

State Comprehensive-Privacy Law Comparison

State	Legislative Process	Statute/Bill (Hyperlinks)	Common Name	Consumer Rights: To Access to Collected	To Access to Shared	To Rectification	To Deletion	To Restriction	To Portability	To Opt-Out	Against Solely Automated Decision Making	Private Right of Action	Business Obligations: Strict Age-based Opt-In	Notice/Transparency Requirement	Data Breach Notification	Risk Assessment	Prohibition on Discrimination	Purpose Limitation	Processing Limitation	Fiduciary Duty
California	Signed	**Ca. Civ. Code §§ 1798.100 - .199**	**California Consumer Privacy Act**	**x**	**x**		**x**		**x**	**x**		**s**	**16**	**x**			**x**			
~~*Connecticut*~~	Introduced	~~*RB 1108/SB 1108*~~																		
Hawaii	In Committee	*SB 418* [I]		*x*	*x*		*x*		*x*	*x*			*16*	*x*	*x*		*x*			
~~*Hawaii*~~	Introduced	~~*HCR 225*~~																		
Illinois	Cross Committee	*HB 3358*	*Data Transparency and Privacy Act*		*x*					*x*				*x*						
~~*Louisiana*~~	Introduced	~~*HB 249*~~																		
Maine	Signed	**LD 946** [II]	**An Act To Protect the Privacy of Online Consumer Information**					**x**		**in**				**x**			**x**			
~~*Maryland*~~	Crossed Chamber	~~*SB 613*~~	~~*Online Consumer Protection Act*~~	~~x~~	~~x~~		~~x~~		~~x~~	~~x~~				~~x~~			~~x~~			
Massachusetts	In Committee	*SD 341/S 120*		*x*	*x*		*x*		*x*	*x*		*x*	*18*	*x*			*x*			
Minnesota	In Committee	*HF 2917/SF 2912*		*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*			*x*		*x*			*x*	
Nevada	Signed	**SB 220/Chapter 603A**								**x**				**x**	**x**					
New Jersey	In Committee	*S2834*			*x*					*x*				*x*			*x*			
~~*New Mexico*~~	Crossed Chamber	~~*SB 176*~~	~~*Consumer Information Privacy Act*~~	~~x~~	~~x~~		~~x~~		~~x~~	~~x~~		~~s~~	~~18~~	~~x~~			~~x~~			
New York	In Committee	*SB S5642* [III]	*New York Privacy Act*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*		*x*	*x*				*x*	*x*
~~*North Dakota*~~	Introduced	~~*HB 1485*~~																		
Pennsylvania	In Committee	*HB 1049*	*Consumer Data Privacy Act*	*x*	*x*		*x*			*x*		*s*	*16*	*x*			*x*			
Rhode Island	In Committee	*HB 5930/S0234*	*Consumer Privacy Protection Act*	*x*	*x*		*x*		*x*	*x*		*x*	*16*	*x*			*x*			
~~*Texas*~~	Introduced	~~*HB 4390*~~ [IV]	~~*Texas Privacy Protection Act*~~																	
Washington	Cross Committee	*SB 5376*	*Washington Privacy Act*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*			*x*	*x*	*x*				

In Session:
MA, NJ, PA

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

Bold - passed law
Italics - proposed bill, not passed
s - private right of action for security violations only
in - opt-in consent requirement

~~Black strikethrough - bill postponed indefinitely~~
~~Purple strikethrough - task force substituted for comprehensive bill~~

[I] Hawaii SB 418 is pending while the task force has been adopted.

[II] Maine LD 946 applies only to internet service providers.

[III] New York SB S5642 includes a broad consumer right to opt-out of any processing, not just the sale of personal information.

[IV] Texas HB 4390 is a GDPR-style restriction-based bill that prohibits a business from collecting or processing information except under certain circumstances.

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

iapp

Last updated: 10/15/2019

Revision of HRS 497-N – Definition of Personal Information

Proposed

"Personal information" means an Identifier in combination with one or more Specified Data Elements.
(i) An Identifier is a common piece of information related specifically to the individual, which is used to identify that individual, such as first name/initial and last name, a user name for an online account, a phone number, or email address.
(ii) "Specified Data Element" means any of the following:

(a) An individual's social security number, either in its entirety or the last four digits.
(b) Driver's license number, federal or state identification card number, or passport number.
(c) An individual's federal or State of Hawaii taxpayer identification number.
(d) An individual's financial account number or credit or debit card number.
(e) A security code, access code, PIN, or password that would allow access to an individual's account.
(f) Health insurance policy number, subscriber identification number, or any other unique number used by a health insurer to identify the person.
(g) Medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid profile.
(h) Unique biometric data generated from a measurement or analysis of human body characteristics used for authentication purposes, such as a fingerprint, voice print, retina or iris image, or other unique physical or digital representation of biometric data.
(i) A digital signature or private key that is unique to an individual and that is used to authenticate or sign an electronic record.

Last 4 of SSN / TIN

- The first three digits are known as the "**Area Number**". Until June 25, 2011, this is generally the State or territory where your SSN was assigned. Thereafter, the number was randomly assigned.
- The second two numbers are known as the "**Group Number**". They really do not have any geographical or data significance.
- The third set of four numbers is simply the numerical sequence of digits 0001 to 9999 issued within each group.

People born in the United States since 1987 may have had their SSN applied for them by the hospital at birth. This policy varies by State.

Hawaii Area Numbers	Group Numbers	
575	01-99	1935 - 2004
576	01-99	1935 - 2004
750	01,03,05,07,09,10,12,14,16,18,20	2004 - 2011
751	01,03,05,07,09,10,12,14,16,18	2004 - 2011

https://www.ssn-verify.com/lookup/hawaii

From IRS.gov

"Examples of PII include, but are not limited to:

a. Name, such as full name, maiden name, mother's maiden name, alias, or name control (first 4 letters of last name).
b. Address information, such as street address or email address.

c. A unique set of numbers or characters assigned to a specific individual, such as:
1. Telephone numbers, including mobile, business, and personal numbers.
2. SSN, including the last 4 digits.
3. Taxpayer identification number (TIN) that identifies an individual."

From HHS.gov (HIPAA)

"a data set that contained … the last four digits of a Social Security number, would not meet the requirement … for de-identification."

Digital Signature

Electronic signatures are a legal concept distinct from **digital signatures**, a cryptographic mechanism often used to implement electronic signatures. While an electronic signature can be as simple as a name entered in an electronic document, digital signatures are increasingly used in e-commerce and in regulatory filings to implement electronic signatures in a cryptographically protected way.

- Arizona: A private key that is unique to an individual and that is used to authenticate or sign an electronic record.

- North Carolina: Digital signatures.

- Alternative wording?
  A digital signature used to create an electronic signature or private key that is unique to an individual and that is used to authenticate or sign an electronic record.

  Or omit digital signature?

Data Brokers

All bills define a data broker as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship

CA AB 1202	Signed by Governor	Requires data brokers to register with and provide certain information to the attorney general. Has a carve out for credit bureaus, financial institutions covered under GLBA, and companies covered by CA's Insurance Information and Privacy Protection Act
IL HB 2871	Pending	Creates the Data Broker Registration Act, requires a data broker to annually register with the secretary of state, defines data broker as a business or unit of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.
ND HB 1524	Failed	Relates to the regulation of data brokers, provides a penalty.
VT H.764	Enacted	Requires data brokers to register with the attorney general. "Data brokers also must disclose annually their practices, if any, for allowing consumers to opt out. Further, the law requires data brokers to report annually the number of data breaches experienced during the prior year and, if known the total number of consumers affected by the breaches." Also requires data brokers to have an Information Security Program. Vermont has a carve out for state agencies. 154 data brokers have registered (as of 11/14/19) https://www.vtsosonline.com/online/DataBrokerInquire/DataBrokerSearch

Geolocation

CA AB 523	Pending	Prescribes the circumstances under which telephone and telegraph corporations may release specified information, including customer proprietary network information, regarding noncommercial subscribers without their written consent. Specifically includes geolocation information in the information that may only be released with a noncommercial subscriber's written consent.
CA Ballot initiative	2020	California Consumer Privacy Rights and Enforcement Act of 2020 Creates a concept of sensitive personal information that includes precise geolocation data. "Precise geolocation" means any data that locates a consumer within a geographic area that is equal to or less than the area of a circle with a radius of half of one mile. https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0017%20%28Consumer%20Privacy%20%29.pdf
CT SB 432	Failed	Expands unfair trade practices to include sale of a customer's global positioning system (GPS) location by mobile phone providers, protects the privacy of mobile telephone users.
HI HB 702	Vetoed	Prohibits the sale or offering for sale of location data collected using satellite navigation technology without the explicit consent of the individual who is the primary user of the satellite navigation technology equipped device.
IL HB 2785	Pending	Creates the Geolocation Privacy Protection Act, defines geolocation information, location-based application, private entity, and user, provides that a private entity may not collect, use, store, or disclose geolocation information from a location-based application on a user's device unless the private entity first receives the person's affirmative express consent after complying with specified notice requirements, provides exceptions, provides that a violation of the act constitutes an unlawful practice.
KY SB 243	Failed	Prohibits telecommunications companies from disclosing or transmitting to a third party any location data derived from a cellular phone without the consent of the customer.
NJ AB 5259	Pending	Prohibits commercial mobile service providers from disclosing a customer's global positioning system data to third parties.
NYC Int 1632-2019	Pending	Prohibits telecommunications carriers and mobile applications from sharing a user’s location data, if the location is within NYC. This bill would also prohibit anyone who receives such location data from sharing it with another person. The penalty would be $1,000 per violation, with a maximum $10,000 per day per person whose location data was unlawfully shared. The Dept. of IT and Telecommunications would enforce. This bill would also create a private right of action.
SC HB 3701	Pending	Enacts the state Cellular Data Privacy Protection Act, defines relevant terms, prohibits a mobile telecommunications provider from selling a customer's personal data to a third party, imposes a penalty, authorizes the attorney general to investigate and enforce alleged violations of this act.

Private Right of Action

Telephone Consumer Protection Act (TCPA) - Federal

Administered by the Federal Communications Commission (FCC) and one of the most frequently litigated statutes, often resulting in national class action litigation.

California Consumer Privacy Act (CCPA)

Effective January 2020, enforced 4/10/20 (6 months after AG issued regulations on 10/10/19)

Limited Private Right of Action for Unauthorized Disclosure of Data: Consumers may bring a private right of action against Covered Businesses in connection with "certain unauthorized access and exfiltration, theft, or disclosure of a consumer's non-encrypted or non-redacted personal information" if the Covered Business has failed to implement and maintain reasonable security measures to protect such information. However, prior to commencing an action for statutory damages (US$100-$750 per incident), the consumer must provide the Covered Business with 30 days to cure the alleged violation and to respond with a written statement that the violation has been cured.

CA AB 1760	Pending	Creates the Privacy for All Act. Prohibits a business from sharing a consumer's personal information unless the consumer has authorized that sharing. Prescribes various business requirements in connection with this new right to opt-in consent. Prohibits discrimination against a consumer based on the exercise of this right. Provides that any violation is an injury and authorizes a consumer to bring suit on this basis.
CA SB 561	Pending	Expands a consumer's rights to bring a civil action for damages to apply to other violations under the California Consumer Privacy Act of 2018. Specifies that the Attorney General may publish materials that provide businesses and others with general guidance on how to comply with the act.

Illinois Biometric Information Privacy Act (BIPA)

The Illinois BIPA is the most stringent biometric privacy law in the U.S for the following reasons:

- It is the only biometrics privacy statute in the country with a private right of action that provides for liquidated damages of up to $5,000 per violation. The term "each violation" is undefined in BIPA and uninterpreted.
- Does not require actual harm. The Illinois Supreme Court in Rosenbach v. Six Flags Entertainment Corp. held that an individual need only prove a technical violation of BIPA and not actual damages. This was extended in Patel v. Facebook Inc., concerning Facebook's use of facial recognition technology used in photo tagging without prior notice and consent and without the required retention schedule.
- BIPA mandates that employers comply with collection, retention, disclosure and destruction protections prior to collecting biometric information as follows:
    - Notice of the collection, the purpose of retention, and storage of biometric information;
    - Acquisition of a written release from individuals to document consent to the collection, storage and use of the biometric information; and
    - Publication of document retention and destruction schedules of biometric information.
- BIPA provisions forbid dissemination, trading, leasing, selling or otherwise profiting from biometric information.
- BIPA, enacted in 2008, does not contain a statute of limitations.
- BIPA contains a HIPAA exemption which applies to patient information
- BIPA has spawned numerous class action lawsuits.

IL SB 2134	Pending	Amends the Biometric Information Privacy Act, deletes language creating a private right of action, provides instead that any violation that results from the collection of biometric information by an

employer for employment, human resources, fraud prevention, or security purposes is subject to the enforcement authority of the Department of Labor, provides that an employee or former employee may file a complaint with the Department alleging a violation.

Right to Deletion

CA AB 288	Pending	Requires a social networking service to provide users that close their accounts the option to have the user's personally identifiable information permanently removed from the company's database and records and to prohibit the service from selling that information to, or exchanging that information with, a third party in the future, subject to specified exceptions. Requires a social media company to honor such a request within a commercially reasonable time.
RI HB 5930	Pending	Creates the Consumer Privacy Protection Act, requires businesses that collect, maintain or sell personal information to notify consumers and would disclose the information and the businesses' use of the information, provides that consumers may opt out and have personal information deleted.

Children's Online Privacy Protection Act (COPPA) - Federal

Applies to minors under the age of 13 and requires that data be deleted when it is no longer "reasonably necessary to fulfill the purpose for which the information was collected."

California Consumer Privacy Act (CCPA)

Effective January 2020, enforced 4/10/20 (6 months after AG issued regulations on 10/10/19)

Under the CCPA, California consumers have a right to request that their personal information be deleted. Covered Businesses must honor "verifiable" requests to delete consumer personal information, subject to several exceptions. Business must also direct their service providers to do the same. Businesses have 45 days to comply with a request, with a 45-day extension.

A business must provide two or more designated methods for submitting requests to delete, including the primary method the business uses to interact with customers.

9 Exceptions

- Transactional - Complete the transaction for which the personal information was collected.
- Security - Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- Errors - Debug to identify and repair errors that impair existing intended functionality.
- Free Speech - Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
- Research in the Public Interest - Engage in public or peer-reviewed scientific, historical, or statistical research.
- Legal Compliance - Comply with a legal obligation.
    - CalECPA Compliance - Comply with the California Electronic Communications Privacy Act.
- Other Internal Uses - Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.
    - Expected Internal Uses - To enable solely internal uses that are reasonably aligned with the expectations of the consumer.

GDPR - Europe

Under GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'.

The right is not absolute and only applies in certain circumstances. Individuals have the right to have their personal data erased if:

- The personal data is no longer necessary for the original purpose;
- The controller/processor relies on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- The controller/processor relies on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- The controller/processor processes the personal data for direct marketing purposes and the individual objects to that processing;
- The controller/processor relies has processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- The controller/processor has to do retain the information to comply with a legal obligation; or
- The controller/processor processed the personal data to offer information society services to a child.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.
- if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational by a health professional).

Businesses must contact entity they shared the data with and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked, the business must also inform the individuals about these recipients.

November 4, 2019

The Honorable Michelle N. Kidani
The Honorable Chris Lee
Hawaii State Capitol
415 South Beretania St
Honolulu, HI 96813

Dear Co-Chairs Kidani and Lee:

TechNet and the Computing Technology Industry Association (CompTIA) appreciate the opportunity to provide preliminary comments regarding the "21st Century Privacy Law Task Force" and offer our assistance to the Task Force moving forward.

TechNet and CompTIA collectively represent the nation's leading technology companies and actively work with our member companies to ensure consumers are provided with reasonable and meaningful privacy policies, while also ensuring new business obligations are clear and workable.

We appreciate Hawaii's commitment through the Task Force to study and examine appropriate laws and regulations related to privacy and stand ready to be a resource to the Task Force. We urge the Task Force not to rush this process. Hawaii has the opportunity to do what other states have not, take the time to develop appropriate and well thought-out privacy legislation. As we have seen in California, a rushed law in 2018 has led to multiple pieces of legislation in 2019 amending the statute, draft regulations that will not be in finalized before the law takes effect and now a new 2020 privacy ballot initiative which has created an incredible amount of uncertainty for consumers and businesses. In contrast, other states, such as Oregon and Rhode Island, have created task forces made up of a variety of stakeholders, including industry, to thoughtfully study the complicated issues within privacy. We urge Hawaii's process follow these models and utilize the

resources of industry and other stakeholders who could provide valuable input to you.

TechNet and CompTIA appreciate the opportunity to provide some initial comments to the 21st Century Task Force and welcome any opportunity to work with you to develop meaningful and clear consumer data privacy legislation. If you have any questions please do not hesitate to contact us at cjensen@technet.org or khitt@comptia.org.

Thank you for your consideration.

Sincerely,

Courtney Jensen
Executive Director, California and the Southwest
TechNet

Kelly Hitt
Senior Director, Government Affairs, California and Hawaii
CompTIA