Information Privacy and Security Council
Meeting Agenda
February 19, 2020
1:00 p.m.

Videoconference Centers (VCC)
Kalanimoku Bldg., 1151 Punchbowl St., Basement B-10, Honolulu, HI 96813
Hilo State Office Bldg., 75 Aupuni St., Basement, Hilo, HI 96720
Wailuku State Office Bldg., 54 S. High St., 3rd Flr., Wailuku, HI 96793
Lihue State Office Bldg., 3060 Eiwa St., Basement, Lihue, HI 96766

I. Call to Order

II. Review and Approval of the December 18, 2019 Meeting Minutes

III. Public Testimony on Agenda Items

Interested persons may submit testimony on any agenda item in writing submitted in advance to Information Privacy and Security Council (IPSC), 1151 Punchbowl St., Room B-10, Honolulu, HI 96813; or email ETS@hawaii.gov, Subject: IPSC Testimony. Each individual or representative of an organization is allotted three minutes for testimony.

IV. House Concurrent Resolution 225, Twenty-first Century Privacy Law Task Force (attached); Discussion and Appropriate Action

V. IT Internal Security Controls

The Council anticipates going into executive session pursuant to HRS section 92-5(a)(6) to consider sensitive matters relating to IT internal security controls.

VI. Good of the Order
a) Announcements
b) Next meeting: March 18, 2020

VII. Adjournment

Individuals who require special needs accommodation are invited to call (808) 586-6000 at least three working days in advance of the meeting.

Information Privacy and Security Council (IPSC)
Meeting Minutes - DRAFT
December 18, 2019

Videoconference Centers (VCC)
Kalanimoku Bldg., 1151 Punchbowl St., Basement B-10, Honolulu, HI 96813
Hilo State Office Bldg., 75 Aupuni St., Basement, Hilo, HI 96720
Wailuku State Office Bldg., 54 S. High St., 3rd Flr., Wailuku, HI 96793
Lihue State Office Bldg., 3060 Eiwa St., Basement, Lihue, HI 96766

Members Present

Vince Hoang, Acting Chair	Office of Enterprise Technology Services (ETS)
Robert Strickland (Designee)	Department of Education (DOE), via VCC Maui*
Gino Merez	Department of Health (DOH)
David Keane	Department of Human Resources Development (DHRD)
Lim Yong	Department of Human Services (DHS)
Kevin Thornton	Judiciary
Jodi Ito (Designee)	University of Hawai‘i (UH)
Karen Sherman	County of Maui, via VCC*
Nyree Norman	County of Kauai, via VCC*
Jules Ung	County of Hawai‘i, via VCC*

* The neighbor island members participated by video and telephone conference.

Members Absent

Stephen Levins	Department of Commerce and Consumer Affairs (DCCA)
Carol Taniguchi	Legislature
Mark Wong	City & County of Honolulu

Other Attendees

Valri Kunimoto	Department of the Attorney General (ATG)
Lori Tanigawa	Department of the Attorney General (ATG)
Kelly McCanlies	Hawaiian Electric Co.
Landon Wong	HPPA

I. Call to Order

Acting Chair Hoang called the meeting to order at 1:11 p.m., at which time quorum was established.

II. Review and Approval of the November 20, 2019 Meeting Minutes

Member Thornton made a motion to approve the November 20, 2019 meeting minutes, which was seconded by Member Keane. A vote was taken and the motion passed unanimously.

III. Public Testimony on Agenda Items

None.

IV. House Concurrent Resolution 225, Twenty-first Century Privacy Law Task Force

The Task Force is considering legislation to revise Chapter 487N, Hawaii Revised Statutes (HRS), concerning the confidentiality of personal information.

Acting Chair Hoang invited Kelly McCanlies, a member of the Task Force, to the meeting. She stated that the Task Force was chaired by Representative Chris Lee and Senator Michelle Kidani. Meetings began in August 2019 and had its last meeting in November. Groups of members worked on ideas that the Task Force wanted to pursue. There are about seven pieces of legislation that were produced by the Task Force but we don't know if all will be introduced. The Task Force's highest priority was revising Chapter 487N, HRS, Security Breach of Personal Information. She shared a draft of the proposed legislation that she will be sending to the Task Force. Most states have updated their laws regarding data breach notification laws, whereas Hawaii has not. She asked the Committee for their input.

Members gave different scenarios asking if the proposed legislation would trigger a data breach. Members questioned whether the definition of an Identifier will erroneously trigger data breach reports. Member Designee Ito felt that the definitions for an Identifier, such as phone number or email address were too broad and most could be considered public information. Ms. McCanlies explained that an Identifier could be used to tie different pieces of information together, which is why its listed that way. She also noted that the current statute also addresses "risk of harm to a person" under the definition of "security breach" so an Identifier with a data element would not automatically be a data breach.

Members subject to HIPAA (Health Insurance Portability and Accountability Act) asked how the proposed changes would affect their reporting when there is a data breach. Ms. McCanlies stated that the current law addresses that issue under Chapter 487N-2(g)2.

Ms. McCanlies stated that about two-thirds of the data breach notification laws have been changed to be more inclusive. Medical identity theft has increased exponentially. The Task Force committee discussed device Identifiers but decided not to include it. It is being considered at the federal level as the Federal Trade Commission stated that device identifiers and especially IP address are now considered personal information.

She plans to submit the proposed draft to the Task Force on Friday. The members can send her an email with their comments before then. Member Thornton recommended changing the last four digits of a Social Security Number to six digits.

V. Good of the Order

a. Announcements: The IPSC will take a recess in January 2020.
b. Next meeting: February 19, 2020

VI. Adjournment

At 2:04 p.m., Member Yong made a motion to adjourn, which was seconded by Member Designee Ito. A vote was taken and the motion passed unanimously.

Recorded by: _____
Susan Bannister, ETS

House Concurrent Resolution No. 225, HD1, SD1 (2019)
Twenty-first Century Privacy Law Task Force

Report to the Legislature

Submitted February 5, 2020.

Contents

Executive Summary

Pursuant to House Concurrent Resolution No. 225, H.D. 1, S.D. 1, (2019), the Twenty-first Century Privacy Law Task Force submits this report to the Hawaii State Legislature.

Through House Concurrent Resolution No. 225, the Legislature found that public use of the internet and related technologies has significantly expanded in recent years, and that a lack of meaningful government regulation has resulted in personal privacy being compromised. Accordingly, the Legislature asked for an examination existing privacy laws and regulations to determine how to protect the privacy interests of the people of Hawaii while meeting or exceeding the existing privacy protections established in the State Constitution and Hawaii Revised Statutes.

The Twenty-first Century Privacy Law Task Force (Task Force) membership consisted of individuals in government and the private sector with an interest or expertise in privacy law in the digital era. The Twenty-first Century Privacy Law Task Force was asked to examine and recommend laws and regulations relating to: internet privacy; the collection, transmission, processing, protection, storage, and sale of personal data; hacking; data breaches; and other similar subjects.

The Task Force's examination into privacy law was conducted in four parts:

1. An assessment of the twenty-first century privacy issues, risks, and laws;
2. Prioritization of specific areas of risk to the privacy of Hawaii residents for deeper discussion and focus;
3. An in-depth examination of the prioritized areas of risk and substantive discussions determining how best to address them; and
4. Formalizing recommendations for legislative action.

The Task Force considered sixteen privacy protections that other jurisdictions have considered or adopted. Of those sixteen protections, Hawaii has currently enacted just one, data breach notification. The sixteen protections include:

- The right of access to personal information collected;
- The right of access to personal information shared with a third party;
- The right to rectification;
- The right to deletion;
- The right to restriction of processing;
- The right to data portability;
- The right to opt-out of the sale of personal information;
- The right against solely automated decision making;
- A consumer private right of action;
- A strict opt-in for the sale of personal information of a consumer less than a certain age;

- Notice/transparency requirements;
- Data breach notification;
- Mandated risk assessment;
- A prohibition on discrimination against a consumer for exercising a right;
- A purpose limitation; and
- A processing limitation.

Additionally, the Task Force considered a spectrum of related privacy issues which have been raised in Hawaii and other states in recent years, including: law enforcement access to personal data; identity theft; the proliferation of deep fake technology; the tracking of a person's real time location; facial recognition technology; and the resale of information by third party data brokers, among others.

While the Task Force recognized the value and importance of meaningfully addressing the sixteen different areas of privacy protections in the long term, it also acknowledged there would not be enough time to conduct a detailed analysis and provide specific recommendations on all sixteen protections and related privacy issue areas given the limited time available to the Task Force. Therefore, the Task Force narrowed the scope of its focus to a limited number of priority areas identified by the Task Force. Following significant inquiry and discussion, the Task Force makes the following recommendations for legislative and regulatory action:

1. *The definition of "personal information" in chapter 487N, Hawaii Revised Statutes, should be updated and expanded.*

2. *Explicit consent should be required before an individual's identifying data can be used for any purpose, shared, or sold. Individuals should have the right to know what data relates to them, the ability to opt in or out of its use, and the right to delete it.*

3. *Explicit consent should be required before an individual's geolocation data can be shared or sold to a third party for monetary or other valuable consideration.*

4. *Explicit consent should be required before an individual's internet browser history and content accessed can be shared or sold to a third party.*

5. *Third party data brokers should be required to register with the State and meaningful tools should be established for people to manage and control their data, including an opt-in or opt-out of the sale or use of their data by third parties. Penalties should be established for non-compliance.*

6. *Hawaii Revised Statutes should be amended to (1) require law enforcement to obtain a search warrant before accessing a person's electronic communications in non-exigent or non-consensual circumstances; and (2) allow a governmental entity to request and a court to approve a request to delay notification of a law enforcement's access to electronic communications no later than the deadline to provide discovery in a criminal case.*

7. *Hawaii should protect the privacy of a person's likeness by adopting laws prohibiting the unauthorized use of deep fake technology.*

Introduction

The Twenty-first Century Digital Privacy Law Task Force (Task Force) was convened and prepared this report pursuant to House Concurrent Resolution No. 225, H.D. 1, S.D. 1 (2019) (hereinafter HCR No. 225).[1] Through HCR No. 225, the Legislature found that public interest usage has significantly expanded in recent years and that a lack of meaningful government regulation has resulted in the privacy of individuals being compromised. Accordingly, the Legislature asked for an examination existing privacy laws and regulations to determine how to protect the privacy interests of the people of Hawaii while meeting or exceeding the existing privacy protections established in the State Constitution and Hawaii Revised Statutes.

Specifically, HCR No. 225 requested the Task Force examine and recommend laws and regulations relating to:

a) Internet privacy;
b) The collection, transmission, processing, protection, storage, and sale of personal data;
c) Hacking;
d) Data breaches; and
e) Other similar subjects.[2]

HCR No. 225 identified individuals who were to serve on the Task Force, and also authorized the Co-Chairs of the Task Force to invite non-listed interested parties to join.[3] Task Force members included:

- Co-Chair of the Task Force, Senator Michelle Kidani (as designated by the President of the Senate);
- Co-Chair of the Task Force, Representative Chris Lee (Chair of the House Committee on Judiciary);
- Deputy Attorney General Bryan Yee (designee of Attorney General Clare Connors);
- Executive Director of the Office of Consumer Protection Stephen Levins (designee of Director of Commerce and Consumer Affairs Catherine Awakuni Colon);
- Chief Information Security Officer Vincent Hoang (designee of Chief Information Officer Douglas Murdock);
- Deputy Prosecuting Attorney Chris Van Marter (designee of Acting Prosecuting Attorney of the City and County of Honolulu);
- Neenz Faleafine, Pono Media (interested party invited by the co-chairs of the Task Force);
- Jay Fidell, ThinkTech Hawaii (interested party invited by the co-chairs of the Task Force);
- Kelly McCanlies, certified privacy expert (interested party invited by the co-chairs of the Task Force);

- Myoung Oh, Charter Communications (interested party invited by the co-chairs of the Task Force); and
- Josh Wisch, ACLU-Hawaii (interested party invited by the co-chairs of the Task Force).

Generally, the Task Force's work was conducted in four parts: (1) the Task Force researched and compiled information related to the current state of data privacy in the United States and elsewhere, heard presentations from stakeholders, and engaged in an initial assessment of the twenty-first century digital privacy issues, risks, and law; (2) the Task Force prioritized specific areas of risk to the privacy of Hawaii residents for deeper discussion; (3) the Task Force compiled in-depth information, received presentations from stakeholders on the prioritized areas of risk, and engaged in substantive discussions about how best to address them; and (4) the Task Force approved recommendations for legislative and regulatory action.

In addition to ongoing research and work done by many stakeholders throughout this time, the Task Force convened in-person on five occasions: August 21, September 26, October 21, November 15, and November 26.[4] Following significant research, discussion, and debate, the Task Force drafted this report and came to the conclusions contained herein, finalizing the document on February 5, 2020.

Examination of twenty-first century privacy laws and regulations

Overview of twenty-first century privacy law issues

Privacy in the digital age of the twenty-first century is a more significant issue for individuals than it has ever been before. The proliferation of online access and reliance on data across government, industries, and everyday life means access to data and violations of privacy can have severe impacts on personal finances, civil liberties, and personal safety.

Technological innovation has made it easier to acquire and use information for improvements to numerous industries such as banking, travel, business, and overall quality of life. However, how that information is gathered, who controls it, and for what purpose it is used have been largely unregulated. As a result, growing incidents and reports in the media in recent years highlight increasing harm to the general public and as the number of unresolved issues and associated risks grow.

Financial scams frequently take advantage of easily accessible personal information. Industries and governments are now frequently able to track and monitor people's location, activities, and interests in real time. Personal information is often collected and used without people's knowledge or consent. Such information is commonly bought and sold by third parties and frequently accessible to bad actors who use it for illicit purposes.

Laws and policies, including those in Hawaii, to ensure privacy protections have been unable to keep pace with the proliferation of new technologies.

To be sure that Task Force members had sufficient baseline knowledge for the examination of digital privacy law, the first meeting of the Task Force was dedicated to examining the topic from a broad perspective.[5] Privacy expert Kelly McCanlies presented an overview of and provided information that examined the state of digital privacy law, including:[6,7]

- Common terms in privacy law;
- Existing federal, state, and local privacy laws;
- Privacy law updates being passed or considered by other jurisdictions;
- The history and provisions of the two major enacted comprehensive privacy laws:
    - General Data Protection Regulation (GDPR), regulating the European Union;[8]
    - California Consumer Privacy Act (CCPA), regulating California;[9]
- Trending privacy issues, including:
    - Facial recognition technology;
    - The sale of geolocation data;
    - Regulations of data brokers;
    - The Internet of Things; and
- An explanation of and comparison of State-laws regarding the sixteen most common provisions to protect personal privacy in the digital age:

- The right of access to personal information collected – "The right for a consumer to access from a business/data controller the information collected or categories of information collected about the consumer; right may only exist if a business sells information to a third party;"[10]
- The right of access to personal information shared with a third party – "The right for a consumer to access personal information shared with third parties;"[11]
- The right to rectification – "The right for a consumer to request that incorrect or outdated personal information be corrected but not deleted;"[12]
- The right to deletion – "The right for a consumer to request deletion of personal information about the consumer under certain conditions;"[13]
- The right to restriction of processing – "The right for a consumer to restrict a business's ability to process personal information about the consumer;"[14]
- The right to data portability – "The right for a consumer to request personal information about the consumer be disclosed in a common file format;"[15]
- 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;"[16]
- 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;"[17]
- A consumer private right of action – "The right for a consumer to seek civil damages from a business for violations of a statute;"[18]
- 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;"[19]
- Notice/transparency requirements – "An obligation placed on a business to provide notice to consumers about certain data practices, privacy operations, and/or privacy programs;"[20]
- Data breach notification – "An obligation placed on a business to notify consumers and/or enforcement authorities about a privacy or security breach;"[21]
- Mandated risk assessment – "An obligation placed on a business to conduct formal risk assessments of privacy and/or security projects or procedures;"[22]
- 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;"[23]
- A purpose limitation – "An EU General Data Protection Regulation–style restrictive structure that prohibits the collection of personal information except for a specific purpose;"[24] and
- A processing limitation – "A GDPR-style restrictive structure that prohibits the processing of personal information except for a specific purpose."[25]

While many of these sixteen protections are in place in numerous states and other countries, in Hawaii only one exists, data breach notification, enacted in 2006.[26]

At its September 26, 2019, meeting, the Task Force received presentations and information regarding the following digital privacy law issues:

- How Hawaii law enforcement has access to electronic communications;[27]
- When a person is notified that Hawaii law enforcement has accessed the person's electronic communications;[28]
- Deep fake technology;[29] and
- Internet Service Provider privacy.[30]

The discussion began with an overview acknowledging that the problems facing Hawaii relating to twenty-first century digital privacy are not Hawaii specific, and that the entire country and world are facing similar problems. Bills have been proposed with varying degrees of success at the federal level, and in various states and municipalities to address the multitude of privacy concerns.

The Task Force also assessed whether the federal, state, or municipal governments are best suited to address these issues. In recent years, Attorneys General and states have tended to favor state action to protect the public, and technology companies have sought favor federal action for cohesiveness. However, it appears unlikely that the federal government will enact any significant legislation addressing the issues in the immediate future.[31] Additionally, considering that federal, state, and municipal governments each have privacy laws in place, it does not appear that there is a jurisdictional problem that prevents the State from passing its own privacy laws, other than limited exceptions for subjects in which existing federal law has preempted state action, such as the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act of 1996, or the Financial Modernization Act of 1999.

Prioritizing areas of risk which should be addressed first

After initial overviews of the breadth of twenty-first century digital privacy issues, the Co-Chairs of the Task Force asked members and interested parties to identify priority areas of risk to Hawaii that the Task Force should more thoroughly examine. The following issues were identified by Task Force members or interested parties, and further information was received, reviewed, and discussed:

- The definition of personal information for Hawaii's data breach notification law;
- Registration and regulation of data brokers;
- Opt-ins or opt-outs for the sale of personal data;
- A private right of action for privacy statute violations;
- Law enforcement's accesses an individual's electronic communications;
- When a person is notified that Hawaii law enforcement has accessed the person's electronic communications;
- Facial recognition technology;
- Deep fake technology;
- The protection of student data and privacy by the State Department of Education;

- Collection and sale of geolocation data;
- The right to deletion; and
- Internet Service Provider privacy.

The following is a summary of the crucial information examined and the discussion surrounding the specific twenty-first century digital privacy areas of risk to Hawaii identified for further examination.

The definition of personal information for Hawaii's data breach notification law

As data is collected digitally, businesses that collect or store data have a responsibility to protect data that is sensitive, confidential, or identifiable from access by hackers, thus exposing persons to identify theft. As of 2018, all fifty states have data breach notification laws that prescribe when consumers must be notified that their data has been breached.[32] Hawaii's data breach notification laws were codified under Chapter 487N, Hawaii Revised Statutes, in 2006. This chapter of Hawaii Revised Statutes, in pertinent parts, defines "personal information" in relation to when a breach notification is required, and specifies the circumstances in which a business or government agency must notify a consumer that their personal information has been breached.[33] When the law was first enacted, it was ahead of the curve because it addressed the relatively new, and quickly escalating, problem of digital-aided identity theft.[34] However, advancements in technology have made digital-aided identity theft easier. Businesses and government agencies now collect more types of data, and bad actors are more able to identify a person with less information, leaving Hawaii's current definition of "personal information" severely outdated and ineffective in preventing harm.[35]

Hawaii's definition of "personal information", which has not been amended or updated since it was enacted, reads:

> "'Personal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
>
> (1) Social security number;
>
> (2) Driver's license number or Hawaii identification card number; or
>
> (3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.
>
> 'Personal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."

In this definition, for a breach notification to be required, a person's name, otherwise known as a piece of information which is an identifier associated with a specific individual, must be breached along with at least one of the three itemized data elements.

The Task Force examined the definitions of personal information from across the country, and focused on the definitions used by eleven states: Arizona,[36] California,[37] Delaware,[38] Illinois,[39] Louisiana,[40] New York,[41] North Carolina,[42] North Dakota,[43] Oregon,[44] Wisconsin,[45] and Wyoming.[46] Each definition is broader than Hawaii's definition of personal information. These definitions both expand the first element of what can constitute an identifier, and include additional options for what is considered a data element.

The Task Force reviewed multiple options and drafts of proposed language to expand Hawaii's definition of personal information, both identifiers and data elements, by amending the law to include components of the various state definitions listed above.[47] Of the identifiers and data elements discussed, specific explanation is required for three specialized data elements in particular, as these components are used in various government documents routinely: (1) the last four digits of a social security number; (2) a tax identification number; and (3) digital signatures.

It was revealed that the last four digits of a social security number are included for protection in various personal information definitions because when the last four digits of a person's social security number are combined with a person's approximate age and place of birth, a bad actor could correctly discover a person's entire social security number approximately one out of fifty times, and with the aid of a simple computer algorithm, an accurate social security number can be deduced in seconds.[48]

It was also revealed that a person's tax identification number, when combined with an identifier, can make a person a target. There was discussion among Task Force members about whether this would implicate State applications that use tax identification numbers.[49] Therefore the proposed legislation was modified to remove the state tax identification number and only include the federal individual tax identification number.

Lastly, Task Force members discussed digital signatures as a specialized data element. It is important to distinguish between an electronic signature and a digital signature. Electronic signatures are a legal concept distinct from digital signatures. Digital signatures are 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.[50]

Registration and regulation of data brokers/Opt-ins or opt-outs for the sale of personal data

The United States Federal Trade Commission has found that:

"Data Brokers Collect Consumer Data from Numerous Sources, Largely Without Consumers' Knowledge: Data brokers collect data from commercial, government, and other publicly available sources. Data collected could include bankruptcy information, voting registration, consumer purchase data, web browsing activities, warranty registrations, and other details of consumers' everyday interactions. Data brokers do not obtain this data directly from consumers, and consumers are thus largely unaware that data brokers are collecting and using this information. While each data broker source may provide only a few data elements about a consumer's activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer's life.

"The Data Broker Industry is Complex, with Multiple Layers of Data Brokers Providing Data to Each Other: Data brokers provide data not only to end-users, but also to other data brokers. The nine data brokers studied obtain most of their data from other data brokers rather than directly from an original source. Some of those data brokers may in turn have obtained the information from other data brokers. Seven of the nine data brokers in the Commission's study provide data to each other. Accordingly, it would be virtually impossible for a consumer to determine how a data broker obtained his or her data; the consumer would have to retrace the path of data through a series of data brokers."

"Data Brokers Collect and Store Billions of Data Elements Covering Nearly Every U.S. Consumer: Data brokers collect and store a vast amount of data on almost every U.S. household and commercial transaction. Of the nine data brokers, one data broker's database has information on 1.4 billion consumer transactions and over 700 billion aggregated data elements; another data broker's database covers one trillion dollars in consumer transactions; and yet another data broker adds three billion new records each month to its databases. Most importantly, data brokers hold a vast array of information on individual consumers. For example, one of the nine data brokers has 3000 data segments for nearly every U.S. consumer."

"Data Brokers Combine and Analyze Data About Consumers to Make Inferences About Them, Including Potentially Sensitive Inferences: Data brokers infer consumer interests from the data that they collect. They use those interests, along with other information, to place consumers in categories. Some categories

> may seem innocuous such as "Dog Owner," "Winter Activity Enthusiast," or "Mail Order Responder." Potentially sensitive categories include those that primarily focus on ethnicity and income levels, such as "Urban Scramble" and "Mobile Mixers," both of which include a high concentration of Latinos and African Americans with low incomes. Other potentially sensitive categories highlight a consumer's age such as "Rural Everlasting," which includes single men and women over the age of 66 with "low educational attainment and low net worths," while "Married Sophisticates" includes thirty-something couples in the "upper-middle class . . . with no children." Yet other potentially sensitive categories highlight certain health-related topics or conditions, such as "Expectant Parent," "Diabetes Interest," and "Cholesterol Focus."
>
> "Data Brokers Combine Online and Offline Data to Market to Consumers Online: Data brokers rely on websites with registration features and cookies to find consumers online and target Internet advertisements to them based on their offline activities. Once a data broker locates a consumer online and places a cookie on the consumer's browser, the data broker's client can advertise to that consumer across the Internet for as long as the cookie stays on the consumer's browser. Consumers may not be aware that data brokers are providing companies with products to allow them to advertise to consumers online based on their offline activities. Some data brokers are using similar technology to serve targeted advertisements to consumers on mobile devices."[51]

In order to protect consumers, jurisdictions are beginning to require a business to offer those they have collected personal information about the option to opt-in or opt-out of the sale of their information to third party data brokers, and for the personal information of children, some laws requires that a parent or guardian to opt-in to the sale of personal information.

Jurisdictions such as Vermont and California have required the registration of regulated data brokers.[52] In California, data brokers are required to register with the office of the state Attorney General, and the Attorney General is responsible for creating a webpage listing registered data brokers.[53] In Vermont, data brokers are required to register with the state Attorney General. Data brokers also must disclose annually their practices for allowing consumers to opt out. The Vermont law also requires data brokers to have an information security program.[54] Furthermore, the Vermont 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.[55]

Vermont law also makes it illegal to acquire information from a data broker for fraud, stalking, harassment, or discrimination pertaining to housing or employment.[56] Enforcement is by the state Attorney General with fines up to $10,000 per year for failure to register.[57] As of November 14, 2019, one-hundred fifty-four data brokers had registered with Vermont.[58]

Data broker registrations allow consumers a chance to know which businesses are collecting personal information for the purpose of selling and sharing that information. A registry of data brokers will allow consumers ease of access in discovering each of the businesses for which the person can opt-out of the sale of their data. California in particular, notes that its data broker registration law assists consumers in utilizing other rights established in the CCPA. In particular, the CCPA establishes the right of consumers to opt-out of the sale of their data. Nevada also has a provision that requires businesses and operators of commercial websites to offer consumers the opportunity to opt-out of the sale of their personal information.[59] Opt-out rights existing in other states are not limited to data brokers.

Legislation to register and regulate data brokers as well as the option for consumers to opt-in or opt-out of the sale of their information has been introduced and is being considered in numerous states.[60,61] California prohibits businesses, including data brokers, from discriminating against consumer that exercise their rights to opt-in or opt-out of the sale of their data or other privacy protections.[62] In California, discrimination includes denying goods or services to a consumer, charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties, providing a different level or quality of goods or services to the consumer, suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.
[63]

The Task Force discussed and reviewed several drafts of proposed legislation that would protect consumers by requiring the registration of data brokers in Hawaii and establishing the right of consumers to opt-in or opt-out of the sale of their data.[64]

A private right of action for privacy statute violations

In the state laws of the United States, private rights of action against business for a breach of a duty to protect a consumer's privacy are generally limited to data breach notification laws. Thought there have been constitutional and negligence claims, in certain jurisdictions where businesses fail to follow data breach notification requirements, consumers have a right to seek civil damages from a business for such violations. In Hawaii, this right is found in section 487N-3(b), Hawaii Revised Statutes:

> "(b) In addition to any penalty provided for in subsection (a),[65] any business that violates any provision of this chapter shall be liable to the injured party in an amount equal to the sum of any actual damages sustained by the injured party as a result of the violation. The court in any action brought under this section may award reasonable attorneys'

fees to the prevailing party. No such action may be brought against a government agency."[66]

Other states that have established a private right of action for violation of data breach notification laws include: Alaska,[67] California,[68] Louisiana,[69] Maryland,[70] Massachusetts,[71] New Hampshire,[72] North Carolina,[73] Virginia,[74] and Washington state.[75] Unlike Hawaii, several of these states do not require demonstration of actual damages to establish a violation of privacy rights in pursuit of a civil action. Moreover, in 2016, the United States Supreme Court supported a broader, less tangible definition of harm for privacy cases than exists in Hawaii law.[76]

The United States Federal government and the European Union have established private rights of action for other privacy-issues. In the United States, a private right of action is included in the federal Telephone Consumer Protection Act that allows a consumer to bring action against non-compliance with automated-dialed or recorded phone calls, faxes, and texts.[77] In the European Union, there is a private right of action in the GDPR for material or non-material damage caused by a data controller or data processors breach of compliance with GDPR.[78]

Legislation in other states has been proposed and is being considered to expand the private right of action to non-data breach notification privacy matters. The Task Force did not review any proposed legislation to establish new private rights of action for privacy matters in Hawaii.

Law enforcement's access to an individual's electronic communications

Currently, in non-exigent circumstances and when it does not have consent, Hawaii's law enforcement must secure a search warrant, court order, or subpoena to require a provider of electronic communication services of remote computing services or of electronic communication service.[79] The greater obtrusion into privacy, the higher the burden on law enforcement to access the information. Specifically, if law enforcement wants to compel disclosure of:

- "Contents" of communications (such as e-mail, text messages, or private comments or tweets), law enforcement must obtain a search warrant;
- "Transactional records" (such as IP logs, cell site data, and e-mail headers), law enforcement must obtain a court order; or
- Call detail records, or subscriber or account user information, law enforcement is permitted to use a subpoena.

In 2018, the United States Supreme Court held in *Carpenter v. United States,* that acquisition of a person's cell-site records was a Fourth Amendment search, and thus required a search warrant for the search to be constitutional.[80]

The Task Force reviewed and discussed proposed legislation to bring Hawaii Revised Statutes in line with the *Carpenter* decision, which eliminates the disparate treatment between "content", "transactional records", and account user records, and treats all forms of electronically

stored data the same by requiring law enforcement to obtain a search warrant to obtain any of these records.[81]

Notification that law enforcement has accessed a person's electronic communications

Hawaii's law enforcement may ask the court to delay disclosure to a user that law enforcement has obtained the user's electronic communications.[82] In practice, the court grants delayed disclosure in close to one hundred percent of the cases involving law enforcement's access to online data.[83] Court-approved non-disclosure orders are based on the need to prevent the harms that are set forth in section 803-47.8(e), Hawaii Revised Statutes. Ultimately, law enforcement discloses their access to electronic communication records as part of the discovery process in criminal cases.[84] The discovery materials, including copies of the legal process and records obtained, are provided to defense counsel and the defendant within ten days of arraignment, pursuant to Rule 16 of the Hawaii Rules of Penal Procedure.[85]

In 2018, the Office of the Prosecuting Attorney of the City and County of Honolulu received 175 search warrants for electronic communications, and the court granted their non-disclosure requests in each circumstance.[86]

The Task Force received and reviewed proposed legislation that would bring section 803-47.8, Hawaii Revised Statutes, up-to date and in line with current law enforcement practices.[87] The proposed legislation retains the judicial discretion provision and requires that disclosure of access to electronic communications be made to the user no later than the deadline for providing discovery in a criminal case.

Facial recognition technology

Facial recognition technology refers to biometric computer programs that analyzes images of human faces for purposes of identifying them. The programs use face templates to analyze distance between eyes, shape of chin, or other face markers, and then compare the analyze to exist images. Facial recognition technology is used by companies such as Facebook[88] and Apple,[89] and has also been used by governments in multiple ways. Additionally, private companies have begun to use facial recognition technology to track and identify people entering their premises.[90]

The United States Department of Homeland Security has been known to use Facial Recognition Technology at our nation's borders as a means to identify known criminals entering the country. Police departments across the country have used facial recognition technology to identify missing children and crime suspects. Most recently in the news, the government of the People's Republic of China, reported to have facial recognition data on all of its 1.4 billion citizens, requires telecom carriers to have and use facial recognition scanners in newly registered mobile devices to track its citizens. Facial recognition technology in China has also drawn media attention when members of the 2019 Hong Kong protests cut down a facial recognition surveillance tower.

In Hawaii, the county police departments use facial recognition technology in a limited capacity in coordination with the Hawaii Criminal Justice Data Center in the office of the Attorney General.[91] Surveillance images from a crime are compared against mugshots already existed in the Hawaii Criminal Justice Data Center's database.[92] The program is intended to identify possible suspects by generating investigative leads for detectives.[93] Facial recognition technology is not currently used to surveil the public to identify or track people in real time.

In the Honolulu Police Department, the technology can only be accessed and used by trained staff, and the results of its use are reviewed by Crime Analysis Unit.[94,95] The technology is only used to compare photographs or video where there is established probable cause, i.e. a photograph of an individual committing a burglary, which compares that image against mugshots from an existing database. If the facial recognition system detects a viable candidate, the Crime Analysis Unit shall complete a follow-up report for the assigned detective.[96] The Crime Analysis Unit analyst's follow-up report shall contain the steps taken to compare the known and unknown photographs and how the Crime Analysis Unit analyst came to their conclusion(s).[97] In the event that a viable candidate cannot be located from the facial recognition system, the assigned detective will be notified that no candidate was identified.[98]

If there is no match in the Honolulu Police Department's facial recognition program, the image may be sent to the FBI to search their Next Generation Identification (NGI) database.[99] Any results from the facial recognition system shall be used only as a guide for the investigation.[100] The information provided does not constitute probable cause for an arrest.[101] The results are only possible name(s) for the photograph(s) and video(s) that were submitted with the request.[102] It shall be the responsibility of the assigned detective to verify the identity of all suspects.[103]

Other jurisdictions in the United States that have enacted laws regulating the use of facial recognition technology include California, San Francisco, Oakland, and Somerville, Massachusetts.

In 2019, California prohibited law enforcement agencies and officers from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera.[104] A person may bring an action for equitable or declaratory relief against a law enforcement agency or officer who violates that prohibition.[105] These provisions repeal on January 1, 2023.[106]

In San Francisco, California, and Somerville, Massachusetts, government acquisition and use of facial recognition technology is prohibited.[107] In Oakland, California, government is prohibited from acquiring, obtaining, retaining, requesting, or accessing facial recognition technology.[108]

In its examination of facial recognition technology, the Task Force heard from ACLU-Hawaii, the Office of the Prosecuting Attorney of the City and County of Honolulu, and the

Honolulu Police Department. ACLU-Hawaii raised concerns about the Constitutionality, disproportionate impacts, and accuracy of facial recognition technology.

ACLU-Hawaii believes that the use of facial recognition technology can implicate First, Fourth, and Fourteenth Amendment privacy rights.[109] In addition, the ACLU cited studies that facial recognition technology disproportionately threatens communities of color and women, as it misidentified ethnic minorities at higher rates, and has a 8.1% -20.6% difference in male to female error rates.[110] And ACLU has concerns about the accuracy of the technology, as it relies on "perfect" conditions (negative results will result from poor lighting, low resolutions, different angle, shadows, backgrounds, poses, facial expressions) and biased datasets.[111]

The Office of the Prosecuting Attorney of the City and County of Honolulu and the Honolulu Police Department emphasized that Hawaii's use of facial recognition technology is only used to identify potential suspects, and that the system has many safeguards.[112] The Office of Prosecuting Attorney also provided the Task Force with reports suggesting the facial recognition technology is more accurate and less biased than the report presented by ACLU-Hawaii.[113]

All parties agreed that facial recognition technology can present benefits but also significant risks, especially if used to identify and track people in real time without their consent. In Hawaii there is currently no statute guiding or restricting the use of facial recognition technology by commercial entities or by law enforcement. No agency is tasked with oversight. Further investigation and discussion on the issue is warranted.

The Task Force did not review any proposed legislation regarding facial recognition technology.

Deep fake technology

Deep fake technology, commonly referred to as deep fakes, is the process of digitally manipulating existing audio and video to depict a person doing or saying something that they did not say or do.[114] Identifying false video and audio employing the use of deep fake technology can be difficult for an unaware viewer. Deep fake technology is widespread enough that even the least technologically inclined persons can easily find and use applications to create false videos. This technology is gaining prevalence for its use in pornography and government, and the people of Hawaii are at risk for both, among other uses.[115]

Deep fake technology that overlays the face or body of one person on another, is increasingly being used to depict individuals as engaging in sexual activity or as performing in the nude without their consent or participation, which can cause economic, reputational, and emotional harm.[116] Individuals, mostly women, are being harassed or exploited online with these videos.[117]

In government, deep fake videos depict politicians such as United States Presidents Barack Obama and Donald Trump saying things they never actually did.[118] Such videos have

circulated widely on the internet. While these examples of deep fake videos have been made explicitly intending the viewer to know that the videos have been altered, a deep fake video of United States House of Representatives Speaker Nancy Pelosi has been shared widely, with numerous online communities and media outlets presenting it as accurate.[119]

In 2019, California enacted a law to address the pornography-associated concerns with deep fake technology.[120] The law creates a private right of action against a person who intentionally distributes a photograph or recorded image of another that exposes the intimate body parts of that person or of a person engaged in a sexual act without the consent of the person depicted.[121]

The Task Force discussed and reviewed proposed legislation from the Office of the Prosecuting Attorney of the City and County of Honolulu and from SAG-AFTRA to amend Hawaii's offense of violation of privacy in the first degree to include scenarios involving the creation and dissemination of deep fake images and videos that use the recognizable physical characteristics of a known person to create a fictitious person depicted in the nude or engaging in sexual conduct.[122]

The protection of student data and privacy by the State Department of Education;

Given the scope of its responsibilities, the State Department of Education collects, processes, and maintains significant amounts of student data. The Office of Technology Services (OTS) within the Department is responsible for the privacy of the information collected. OTS "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."[123] OTS gave a presentation to the Task Force and explained the varied ways that student data is protected.[124]

In addition to examining how student data and privacy are protected institutionally, the Task Force considered how students are being taught privacy matters. The Department of Education explained in part:

"There is no established curriculum or course work that addresses privacy training or privacy awareness to the general student population. However, some advisory information is being disseminated through various Computer Science media courses. Additionally, [the Office of Curriculum, Instruction and Student Support Department] has been going out with a presentation to teachers on Digital Literacy that incorporates information on online awareness and safety. They reference [the State Department of Education's] "Internet Safety" webpage as an additional resource."[125]

The Task Force did not review any proposed legislation to address or alter the way the State Department of Education protects student data or privacy.

Collection and sale of geolocation data

Geolocation data, information that can accurately identify a person's physical location, is routinely collected by mobile devices, such as smartphones, tablets, personal computers, vehicles, and smartwatches; and applications of the devices, such as maps, browsers, cameras, social media, and sometimes even unexpected applications with no relevant need for location data such as a particular flashlight application on a mobile phone. The location of a particular device is typically collected and made available in real time or with just minutes of delay.

Certain businesses sell geolocation data to third parties without the knowledge or consent of the user. When geolocation data is collected from a smartphone or other device that people tend to keep on or near their person, the geolocation data becomes a permanent record of a person's movement and daily life. Although many companies that share, sell, or purchase geolocation data utilize anonymized data, that is, data unattached to a specific person's name, the tracking is so precise that an anonymous person can easily be identified, i.e. by monitoring which devices are present at a particular address, during a commute to a particular school, or in a specific place at a specific time.

Identifying a person's real time location and allowing them to be tracked without their knowledge or consent by third parties who share or sell their real time location creates serious privacy and safety concerns. For example, visitors to particular abortion clinics or churches can be tracked to their home addresses and identified. A stalker could acquire and track the real time location of a victim. And alarmingly, a New York Times investigation revealed that it was easily able to track the real time location of President Donald Trump by following the real time location data of devices associated with members of the Secret Service.[126]

Numerous states have or are considering some form of legislation to regulate or prohibit the sale of geolocation data, including California,[127] Connecticut,[128] Hawaii,[129] Illinois,[130] Kentucky,[131] New Jersey,[132] New York City,[133] and South Carolina.[134]

The Task Force discussed and reviewed proposed legislation that would prohibit the sale of geolocation data without explicit consent.[135]

The right to deletion

In the twenty-first century, people are sharing more of their life and information on the internet, and businesses are collecting and maintaining extensive information on internet users. "The right to deletion" refers to common privacy provision in which a consumer can request the deletion of their personal information under certain conditions.[136] Right to deletion provisions have been passed by the United States Congress, the European Union, and California.

At the federal level, the Children's Online Privacy Protection Act requires that data collected from minors under the age of thirteen must be deleted when it is no longer reasonably necessary to fulfill the specific purposes for which the information was collected.[137]

Residents of European Union have the right to have personal data erased.[138] This is known as the right to erasure or 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:[139]

- The personal data is no longer necessary for the original purpose;
- The controller/processor relies on consent as its lawful basis for holding the data, and the individual withdraws their consent;
- The controller/processor relies on legitimate interests as its 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;
- The controller/processor has 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:[140]

- 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;
- For the establishment, exercise, or defense of legal claims;
- If the processing is necessary for public health purposes in the public interest (e.g. 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 medicinal care by a health professional.

Additionally, businesses must contact each 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.[141]

Effective January 1, 2020, and enforced July 1, 2020, 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 forty-five days to comply with a request and may receive an additional forty-five-day extension.

A business must provide two or more designated methods for consumers to submit requests to delete, including the primary method the business uses to interact with customers.[142]

There are nine exceptions to when a business does not need to fulfill a request to delete personal information, including if the business needs the personal information to:[143]

- Complete the transaction for which the personal information was collected;
- To detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or to prosecute those responsible for that activity;
- Debug to identify and repair errors that impair existing intended functionality;
- 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;
- Engage in public or peer-reviewed scientific, historical, or statistical research;
- Comply with a legal obligation;
- Comply with the California Electronic Communications Privacy Act;
- Use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information; or
- Enable solely internal uses that are reasonably aligned with the expectations of the consumer.

Various right to deletion provisions have additionally been proposed and are being considered in states such as Connecticut, Hawaii, Maryland, Massachusetts, Minnesota, New Mexico, New York, Pennsylvania, Rhode Island, Texas, and Washington state.[144]

The Task Force discussed and considered proposed legislation on the issue as part of proposed legislation regulating data brokers.[145]

Internet Service Provider privacy

An Internet Service Provider (ISP) is a company such as AT&T, Verizon, Spectrum, or Comcast, which provides Internet access to companies, families, and individuals, both hardwired and mobile users. ISPs use fiber-optics, satellite, copper wire, and other forms to provide Internet access to its customers.[146] The average customer must use an ISP to access the internet, and ISPs have the ability to track and record personal information, such as web browsing activity, of a user of its services, although ISPs currently lack the ability of search engines, social networking platforms, and others in the internet ecosystem to tack users' activity across multiple networks and devices.[147] In 2017, President Donald Trump signed a congressional resolution that repealed ISP-specific privacy rules adopted by the Federal Communications Commission that had yet to go into effect which, in part, would have banned ISPs from to selling non-identifying personal information to third parties.[148]

Jurisdictions that have placed restrictions on ISPs include Minnesota, Nevada, and Maine.[149] Nevada and Minnesota passes their laws in 1999 and 2002 respectively, and Maine passed its ISP-specific privacy law in 2019.

Minnesota's law:[150]

- Prohibits ISPs from sharing personal identifying information without consent or for subpoena, court order, or search warrant;
- Requires ISPs to have reasonable security; and
- Allows an individual to bring action with awards of $500 or actual damage.

Nevada's law:[151]

- Applies to provider who charges for internet service or electronic mail address
- ISPs must keep all information confidential all information (other than email address) unless consent is given;
- ISPs may share email addresses unless consent is withdrawn; and
- Violations of the section are misdemeanor, with a fine of $50 - $500 per violation.

Maine's law:[152]

- Prohibits a provider of broadband Internet access service from using, disclosing, selling, or permitting access to customer personal information unless the customer expressly consents to such; and
- Provides other exceptions under which a provider may use, disclose, sell, or permit access to customer personal information, prohibits a provider from refusing to serve a customer, charging a customer a penalty, or offering a customer a discount.

Jurisdictions that have introduced, are considering, or considered laws regulating ISP privacy include: Connecticut,[153] Hawaii,[154] Louisiana,[155] Maryland,[156] Massachusetts,[157] Montana,[158] New Jersey,[159] New York,[160] and South Carolina.[161]

The Task Force discussed legislation that would prohibit the sharing and sale of web browser history and online activity, with focus on legislation applying not just to internet service providers, but to everyone. The Task Force did not review any legislation on the subject.

Recommendations

The Twenty-first Century Privacy Law Task Force recognizes that successfully protecting the digital privacy, civil rights, and safety of the people of Hawaii is not achievable with a single piece of legislation or with the recommendations of a single Task Force. Technology, society, and the ways in which information is used are constantly evolving, creating new privacy concerns with each passing year.

The Task Force recognizes the value and importance of meaningfully addressing the full spectrum of the sixteen basic areas of privacy protections identified to ensure Hawaii residents' digital privacy, civil rights, and safety are protected. However, due to its limited time and resources, the Task Force was unable to conduct a deep dive and provide specific recommendations on all sixteen protections and related privacy issue areas. The Task Force was only able to thoroughly examine certain topics which it felt were of the highest priority or which allowed for clear solutions. Accordingly, while the Task Force makes the following specific recommendations based on its examination of twenty-first century privacy laws, it recognizes that these recommendations do not comprehensively address the full scope of current and growing privacy risks facing residents of Hawaii.

Therefore, to protect the digital privacy of the people of Hawaii, policymakers, government officials, and the public should address the areas of digital privacy and sixteen basic protections this Task Force did not address, and broadly and thoroughly engage in an ongoing examination of digital privacy to keep pace with rapidly evolving technology and its uses in the twenty-first century.

The definition of "personal information" in chapter 487N, Hawaii Revised Statutes, should be updated and expanded.

Hawaii's definition of personal information is outdated and needs to be updated. There are too many identifying data elements which when exposed to the public in a data breach, place an individual at risk of identity theft or may compromise their personal safety. Hawaii's current law which requires the public to be notified of data breaches is not comprehensive enough to cover the additional identifiers. The Task Force recommends that the definition of personal information be updated and expanded to include various personal identifiers and data elements which are found in more comprehensive laws.

The following is proposed language reviewed by the Task Force to achieve this recommendation:

"SECTION xx. Section 487N-1, Hawaii Revised Statutes, is amended by adding two new definitions to be appropriately inserted and to read as follows:

'"Identifier" means a common piece of information related specifically to the individual, which is commonly used to identify that individual across technology platforms, such as, but not limited to, first name, initial, and last name, a user name for an online account, a phone number, or an email address.

"Specified data element" means any of the following:

(1) An individual's social security number, either in its entirety or the last four or more digits;

(2) Driver's license number, federal or state identification card number, or passport number;

(3) A federal individual taxpayer identification number;

(4) An individual's financial account number or credit or debit card number;

(5) A security code, access code, PIN, or password that would allow access to an individual's account;

(6) Health insurance policy number, subscriber identification number, or any other unique number used by a health insurer to identify a person;

(7) Medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid profile;

(8) 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; and

(9) A private key that is unique to an individual and that is used to authenticate or sign an electronic record.'

SECTION xx. Section 487N-1, Hawaii Revised Statutes, is amended by amending the definition of "personal information" to read as follows:

"Personal information" means an [~~individual's first name or first initial and last name in combination with any one or more of the~~

~~following data elements, when either the name or the data elements are not encrypted:~~

~~(1) Social security number;~~

~~(2) Driver's license number or Hawaii identification card number; or~~

~~(3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.~~]

identifier in combination with one or more specified data elements."

Explicit consent should be required before an individual's identifying data can be used for any purpose, shared, or sold. Individuals should have the right to know what data relates to them, the ability to opt in or out of its use, and the right to delete it.

The Task Force discussed the idea that an individual's identifying data can be used, sold, and purchased without consent, but given its time constraints, did not review proposed specific legislation on the subject. This is a significant privacy risk to those that do not know that such practices take place. The Task Force believes that legislation should be enacted allowing Hawaii citizens to know what data is being collected about them, to opt-in or opt-out of the collection of that data, and be ensured the right to delete that data.

Explicit consent should be required before an individual's geolocation data can be shared or sold to a third party for monetary or other valuable consideration .

Identifying a person's real time location and allowing them to be tracked without their knowledge or consent by third parties who share or sell their real time location creates serious privacy and safety concerns. The Task Force recommends that explicit consent should be required before an individual's geolocation data can be shared or sold to a third party.

The following is proposed language reviewed by the Task Force to achieve this recommendation:

"SECTION xx. Chapter 481B, Hawaii Revised Statutes, is amended by adding a new section to part I to be appropriately designated and to read as follows:

'**§481B- Sale of geolocation data without consent is prohibited.** (a) No person shall, in any manner, or by any

means, sell or offer for sale geolocation data that is recorded or collected through any means by mobile devices or location-based applications without the explicit consent of the individual who is the primary user of the device or application.

(b) As used in this section:

"Consent" means prior express opt-in authorization which may be revoked by the user at any time.

"Geolocation information" means information that is:

(1) Not the contents of a communication;

(2) Generated by or derived from, in whole or in part, the operation of a mobile device, including, but not limited to, a smart phone, tablet, fitness tracker, e-reader, or laptop computer; and

(3) Sufficient to determine or infer the precise location of the user of the device.

"Precise location" means any data that locates a user within a geographic area that is equal to or less than the area of a circle with a radius of one mile.

"Location-based application" means a software application that is downloaded or installed onto a device or accessed via a web browser and collects, uses, or stores geolocation information.

"Sale" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a user's geolocation information to another business or a third party for monetary or other valuable consideration.

"User" means a person who purchases or leases a device, or installs or uses an application on a mobile device.

Explicit consent should be required before an individual's internet browser history and content accessed can be shared or sold to a third party.

The Task Force discussed prohibiting the sharing and sale of web browser history and online activity by anyone in Hawaii, but given its time constraints, did not review any specific proposed legislation on the subject. The Task Force believes that legislation should be enacted protecting a person's internet browsing and content access history, in a new standalone provision similar to the recommended language relating to the sale of geolocation data and the sale of personal information.

Third party data brokers should be required to register with the State and meaningful tools should be established for people to manage and control their data, including an opt-in or opt-out of the sale or use of their data by third parties. Penalties should be established for non-compliance.

Requiring a registry of data brokers will allow consumers to know which businesses are gathering and selling information on them and provide a pathway to opt-out of the sale of their data by the data brokers who have registered. The Task Force believes that requiring data brokers to register with the State will only be effective if there are other components attached to the registration that consumers can use to learn of, control, and manage their data, and if there are penalties attached for non- compliance with registration.

The following is proposed language reviewed by the Task Force to achieve this recommendation:

"SECTION xx. Chapter 487N, Hawaii Revised Statutes, is amended by adding a new part to be appropriately designated to read as follows:

'PART . DATA BROKERS

§487N-A Annual registration. (a) Annually, on or before January 31, following a year in which a business meets the definition of data broker, a data broker shall:

(1) Register with the office of consumer protection;

(2) Pay a registration fee of $100.00; and

(3) Provide the following information to the office of consumer protection:

(A) The name and primary physical, e-mail, and internet addresses of the data broker;

(B) If the data broker permits a consumer to opt-out of the data broker's collection of personal information, opt-out of its databases, or opt-out of certain sales of data:

(i) The method for requesting an opt-out;

(ii) Which activities and sales the opt-out applies to; and

(iii) Whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer’s behalf;

(C) A statement specifying the data collection, databases, or sales activities from which a consumer may not opt out;

(D) A statement whether the data broker implements a purchaser credentialing process;

(E) The number of security breaches that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches;

(F) Where the data broker has actual knowledge that it possesses the personal information of minors, a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the personal information of minors; and

(G) Any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(b) A data broker that fails to register shall be subject to:

(1) A civil penalty of $100.00 for each day it fails to register pursuant to this section;

(2) An amount equal to the fees due under this section during the period it failed to register pursuant to this section; and

(3) Other penalties imposed by law and expenses incurred by the attorney general in the investigation and

prosecution of the action, as the court deems appropriate.

(c) The attorney general may take legal action to collect or cause the collection of the penalties, fees and other moneys imposed in this section and to seek appropriate injunctive relief.

(d) The office of consumer protection shall create a page on its internet website where the information provided by data brokers under this title shall be accessible to the public.

§487N-B Duty to protect personal information. (a) A data broker shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the:

(1) Size, scope, and type of business of the data broker obligated to safeguard the personal information under such comprehensive information security program;

(2) Amount of resources available to the data broker;

(3) Amount of stored data; and

(4) Need for security and confidentiality of personal information.

(b) A data broker subject to this part shall adopt safeguards in the comprehensive security program that are consistent with the safeguards for protection of personal information and information of a similar character set forth in other State rules or federal regulations applicable to the data broker. A comprehensive information security program shall at minimum have the following features:

(1) Designation of one or more employees to maintain the program;

(2) Identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personal information, and a process for evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including:

(A) Ongoing employee training, including training for temporary and contract employees;

(B) Employee compliance with policies and procedures; and

(C) Means for detecting and preventing security system failures;

(3) Security policies for employees relating to the storage, access, and transportation of records containing personal information outside business premises;

(4) Disciplinary measures for violations of the comprehensive information security program rules;

(5) Measures that prevent terminated employees from accessing records containing personal information;

(6) Supervision of service providers, by:

(A) Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with applicable law; and

(B) Requiring third-party service providers by contract to implement and maintain appropriate security measures for personal information;

(7) Reasonable restrictions upon physical access to records containing personal information and storage of the records and data in locked facilities, storage areas, or containers;

(8) Regular monitoring to:

(A) Ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and

(B) Upgrade information safeguards as necessary to limit risks;

(9) Regular review of the scope of the security measures must occur:

(A) At least annually; or

(B) Whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information; and

(10) Documentation of responsive actions taken in connection with any incident involving a breach of security, and post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

§487N-C Computer system security requirements. A comprehensive information security program required by this

section shall at minimum, and to the extent technically feasible, have the following elements:

(1) Secure user authentication protocols that have the following features; provided that in lieu of the requirements, an authentication protocol providing a higher level of security may be used:

(A) Control of user IDs and other identifiers;

(B) A reasonably secure method of assigning and selecting passwords or use of unique identifier technologies, such as biometrics or token devices;

(C) Control of data security passwords to ensure that such passwords are kept in a location and format that do not compromise the security of the data they protect;

(D) Restricting access to only active users and active user accounts; and

(E) Blocking access to user identification after multiple unsuccessful attempts to gain access;

(2) Secure access control measures that:

(A) Restrict access to records and files containing personal information to those who need such information to perform their job duties; and

(B) Assign to each person with computer access unique identifications plus passwords, which are not vendor-supplied default passwords, that are reasonably designed to maintain the integrity of the security of the access controls or a protocol that provides a higher degree of security;

(3) Encryption of all transmitted records and files containing personal information that will travel across public networks and encryption of all data containing personal information to be transmitted wirelessly or a protocol that provides a higher degree of security;

(4) Reasonable monitoring of systems for unauthorized use of or access to personal information;

(5) Encryption of all personal information stored on laptops or other portable devices or a protocol that provides a higher degree of security;

(6) For files containing personal information on a system that is connected to the internet, reasonably up-to-

date firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personal information or a protocol that provides a higher degree of security;

(7) Reasonably up-to-date versions of system security agent software that includes malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions and is set to receive the most current security updates on a regular basis or a protocol that provides a higher degree of security; and

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

§487N-D Acquisition, use, and sale of personal information; prohibitions. (a) A person shall not acquire personal information through fraudulent means.

(b) A person shall not acquire or use personal information for the purpose of:

(1) Stalking or harassing another person;

(2) Committing a fraud, including identity theft, financial fraud, or email fraud; or

(3) Engaging in unlawful discrimination, including employment discrimination and housing discrimination.

(c) Any data broker, which is not a consumer reporting agency, shall establish a designated request process through which a consumer may submit a request pursuant to this part. A consumer may, at any time, submit a request through a designated request process to a data broker directing the data broker not to make any sale of any covered information the data broker has collected or will collect about the consumer.

(d) A data broker that has received a request submitted by a consumer shall not make any sale of any covered information the data broker has collected or will collect bout that consumer.

(e) A data broker shall respond to a request submitted by a consumer within sixty days after receipt. A data broker may extend by not more than thirty days the period prescribed by this subsection if the operator determines that such an extension is reasonably necessary. An operator who extends the period prescribed by this subsection shall notify the consumer of such an extension.

§487N-E Disclosures to consumers. (a) A data broker shall, upon request and proper identification of any consumer, clearly and accurately disclose to the consumer all information that the data broker has collected at the time of the request pertaining to the consumer, including:

(1) The categories of personal information it has shared about that consumer;

(2) The categories of sources from which the personal information is collected;

(3) The names of third parties with whom the data broker has shared personal information during the prior twelve-month period and the date of each request; and

(4) The specific pieces of personal information it has shared about that consumer.

(b) A data broker may provide disclosure to a consumer at any time, but shall not be required to provide disclosure to a consumer more than twice in a twelve-month period.

(c) Consumer reporting agencies that broker data of residents of the State shall annually provide a written notice to consumers, in at least twelve point type, containing the following information:

(1) The circumstances under which a consumer has the right to receive a free copy of their credit report and the methods for obtaining the report;

(2) The circumstances under which a person may access another person's credit report without their permission, such as in response to a court order, or direct mail offers of credit;

(3) An explanation of a security freeze, along with the circumstances under which the consumer has the right to place a "security freeze" on a credit report, and the costs and process for placing the freeze; and

(4) Notice that if the consumer believes a law regulating consumer credit reporting has been violated, they may file a complaint with the Federal Trade Commission, with the processes for filing the complaint.

§487N-F Discrimination against consumers. (a) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this part, including, but not limited to, by:

(1) Denying goods or services to the consumer;

(2) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;

(3) Providing a different level or quality of goods or services to the consumer;

(4) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(b) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

(c) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data.

§487N-G Enforcement; penalties. (a) A person who violates a provision of this part other than section 487N-A, shall be subject to the offense of a deceptive business practice as provided in HRS 480-2.

(b) The attorney general may adopt rules to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, and bring civil actions as provided by law.'

SECTION xx. Section 487N-1, Hawaii Revised Statutes, is amended by adding five definitions as follows:

'"Consumer" means an individual residing in the State of Hawaii.

"Consumer Reporting Agency" shall have the same meaning as the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

"Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the personal information of a consumer with whom the business does not have a direct relationship.

"Direct relationship" means a relationship, past or present, between a consumer and a business in which the consumer is: a customer, client, subscriber, or user of the business's goods or services; employee, contractor, or agent of the business; investor in the business; or donor to the business.

"Direct relationship" does not include activities conducted by a business, and the collection and sale or licensing of personal information incidental to conducting these activities, do not qualify the business as a data broker:

(1) Developing or maintaining third-party e-commerce or application platforms;

(2) Providing directory assistance or directory information services, including name, address, and

telephone number, on behalf of or as a function of a telecommunications carrier;

(3) Providing publicly available information related to a consumer's business or profession; or

(4) Providing publicly available information via real-time or near real-time alert services for health or safety purposes.

"License" means a grant of access to, or distribution of, data by one business to another in exchange for consideration. Sharing of data for the sole benefit of the business providing the data, where that business maintains sole control over the use of the data, is not a license.

"Sells or licenses" does not include:

(1) A one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or

(2) A sale or license of data that is merely incidental to the business.'

SECTION xx. Chapter 487N, Hawaii Revised Statutes, is amended by amending its title to read as follows:

'CHAPTER 487N

[~~[SECURITY BREACH~~] PRIVACY OF PERSONAL INFORMATION[~~]~~]'"

Hawaii Revised Statutes should be amended to (1) require law enforcement to obtain a search warrant before accessing a person's electronic communications in non-exigent or non-consensual circumstances; and (2) allow a governmental entity to request and a court to approve a request to delay notification of a law enforcement's access to electronic communications no later than the deadline to provide discovery in a criminal case.

Considering the holding in *Carpenter v. United States,* the Task Force recommends amending Hawaii Revised Statutes to require law enforcement to obtain a search warrant prior to accessing a person's electronic communications in non-exigent or non-consensual circumstances. In order to align statute with current practices, the Task Force recommends amending Hawaii Revised Statutes to allow governmental entities to request and courts to approve a request to delay notification of a law enforcement's access to electronic communications no later than the deadline to provide discovery in a criminal case.

The following is proposed language reviewed by the Task Force to achieve this recommendation:

"SECTION xx. Section 803-41, Hawaii Revised Statutes, is amended by adding a definition of "Electronically stored data" to be appropriately designated and to read as follows:

'"Electronically stored data" means any information that is recorded, stored, or maintained in electronic form by an electronic communication service or a remote computing service, and includes, but is not limited to, the contents of communications, transactional records about communications, and records and information that relate to a subscriber, customer, or user of an electronic communication service or a remote computing service.'

SECTION xx. Chapter 803-47.6, Hawaii Revised Statutes, is amended to read as follows:

"**§803-47.6 Requirements for governmental access.** (a) [~~A~~] Except as otherwise provided by law, a governmental entity may require [~~the disclosure by~~] a provider of an electronic communication service [~~of the contents of an electronic communication~~] and a provider of a remote computing service to disclose electronically stored data pursuant to a search warrant [~~only~~] or written consent from the customer, subscriber, or user of the service.

[~~(b) A governmental entity may require a provider of remote computing services to disclose the contents of any electronic communication pursuant to a search warrant only.~~

~~(c) Subsection (b) of this section is applicable to any electronic communication held or maintained on a remote computing service:~~

~~(1) On behalf of, and received by electronic transmission from (or created by computer processing of communications received by electronic transmission from), a subscriber or customer of the remote computing service; and~~

~~(2) Solely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access~~

~~the contents of those communications for any purpose other than storage or computer processing.~~

~~(d)(1) A provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to, or customer of, the service (other than the contents of any electronic communication) to any person other than a governmental entity.~~

~~(2) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to, or customer of, the service (other than the contents of an electronic communication) to a governmental entity only when:~~

~~(A) Presented with a search warrant;~~

~~(B) Presented with a court order, which seeks the disclosure of transactional records, other than real-time transactional records;~~

~~(C) The consent of the subscriber or customer to the disclosure has been obtained; or~~

~~(D) Presented with an administrative subpoena authorized by statute, an attorney general subpoena, or a grand jury or trial subpoena, which seeks the disclosure of information~~

~~concerning electronic communication, including but not limited to the name, address, local and long distance telephone billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of the service, and the types of services the subscriber or customer utilized.~~

~~(3) A~~] (b) Unless otherwise authorized by the court, a governmental entity receiving records or information under this [~~subsection~~] section is [~~not~~] required to provide notice to [~~a~~] the subscriber [~~or~~], customer, or user of the service.

[~~(c) A court order for disclosure under subsection (d) shall issue only if the governmental entity demonstrates probable cause that the records or other information sought, constitute or relate to the fruits, implements, or existence of a crime or are relevant to a legitimate law enforcement inquiry. An order may be quashed or modified if, upon a motion promptly made, the service provider shows that compliance would be unduly burdensome because of the voluminous nature of the information or records requested, or some other stated reason establishing such a hardship.~~]

[~~(f)~~] (c) No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified

persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, or subpoena.

[~~(g)~~] (d) A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a [~~court order or other process~~] search warrant. Records shall be retained for a period of ninety days, which shall be extended for an additional ninety-day period upon a renewed request by the governmental entity."

SECTION xx. Section 803-47.7, Hawaii Revised Statutes, is amended as follows:

1. By amending subsection (a) to read:

'(a) A governmental entity may include in its [~~court order~~] search warrant a requirement that the service provider create a backup copy of the contents of the electronic communication without notifying the subscriber or customer. The service provider shall create the backup copy as soon as practicable, consistent with its regular business practices, and shall confirm to the governmental entity that the backup copy has been made. The backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.'

2. By amending subsection (e) to read:

'(e) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (b) of this section, the subscriber or customer may file a motion to vacate the [~~court order~~] search warrant, with written notice and a copy of the motion being served on both the governmental entity and the service provider. The motion to vacate a [~~court order~~] search warrant shall be filed with the designated judge who issued the [~~order~~] warrant. The motion or application shall contain an affidavit or sworn statement:

(1) Stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications are sought; and

(2) Setting forth the applicant's reasons for believing that the records sought does not constitute probable cause or there has not been substantial compliance with some aspect of the provisions of this part.'

3. By amending subsection (g) to read:

'(g) If the court finds that the applicant is not the subscriber or customer whose communications are sought, or that there is reason to believe that the law enforcement inquiry is legitimate and the justification for the communications sought is supported by probable cause, the application or motion shall be denied, and the court shall order the release of the backup

copy to the government entity. A court order denying a motion or application shall not be deemed a final order, and no interlocutory appeal may be taken therefrom by the customer. If the court finds that the applicant is a proper subscriber or customer and the justification for the communication sought is not supported by probable cause or that there has not been substantial compliance with the provisions of this part, it shall order vacation of the [~~order~~] warrant previously issued.'

SECTION xx. Section 803-47.7, Hawaii Revised Statutes, is amended as follows:

1. By amending subsection (a) to read:

'(a) A governmental entity may as part of a request for a [~~court order~~] search warrant include a provision that notification be delayed for a period not exceeding ninety days or, at the discretion of the court, no later than the deadline to provide discovery in a criminal case, if the court determines that notification of the existence of the court order may have an adverse result.'

2. By amending subsection (c) to read:

'(c) Extensions of delays in notification may be granted up to ninety days per application to a court or, at the discretion of the court, up to the deadline to provide discovery in a criminal case. Each application for an extension must comply with subsection (e) of this section.'

3. By amending subsection (e) to read:

'(e) A governmental entity may apply to the designated judge or any other circuit judge or district court judge, if a circuit court judge has not yet been designated by the chief justice of the Hawaii supreme court, or is otherwise unavailable, for an order commanding a provider of an electronic communication service or remote computing service to whom a search warrant, or court order is directed, not to notify any other person of the existence of the search warrant[~~, or court order~~] for such period as the court deems appropriate not to exceed ninety days or, at the discretion of the court, no later than the deadline to provide discovery in a criminal case. The court shall enter the order if it determines that there is reason to believe that notification of the existence of the search warrant[~~, or court order~~] will result in:

(1) Endangering the life or physical safety of an individual;

(2) Flight from prosecution;

(3) Destruction of or tampering with evidence;

(4) Intimidation of potential witnesses; or

(5) Otherwise seriously jeopardizing an investigation or unduly delaying a trial.'"

Hawaii should protect the privacy of a person's likeness by adopting laws prohibiting the unauthorized use of deep fake technology.

Technology is improving rapidly, and social media makes it simple to share content. The effects of deep fake technology on the personal and societal level can be personally and politically far reaching. The Task Force recommends establishing criminal violations for those who violate a person's privacy by creating deep fake videos including their likeness without their consent.

The following is proposed language reviewed by the Task Force to achieve this recommendation:

"SECTION xx. Section 711-1110.9, Hawaii Revised Statutes, is amended to read as follows:

'**§711-1110.9 Violation of privacy in the first degree.** (1) A person commits the offense of violation of privacy in the first degree if, except in the execution of a public duty or as authorized by law:

(a) The person intentionally or knowingly installs or uses, or both, in any private place, without consent of the person or persons entitled to privacy therein, any device for observing, recording, amplifying, or broadcasting another person in a stage of undress or sexual activity in that place; [~~or~~]

(b) The person knowingly discloses or threatens to disclose an image or video of another identifiable person either in the nude, as defined in section 712-1210, or engaging in sexual conduct, as defined in section 712-1210, without the consent of the depicted

person, with intent to harm substantially the depicted person with respect to that person's health, safety, business, calling, career, education, financial condition, reputation, or personal relationships or as an act of revenge or retribution; [~~provided that:~~] or

(c) The person intentionally creates or discloses, or threatens to disclose, an image or video of a fictitious person depicted in the nude, as defined in section 712-1210, or engaged in sexual conduct, as defined in section 712-1210, that includes the recognizable physical characteristics of a known person such that the image or video appears to depict the known person and not a fictitious person, with intent to harm substantially the depicted person with respect to that person's health, safety, business, calling, career, education, financial condition, reputation, or personal relationships, or as an act of revenge or retribution.

[~~(i)~~] (2) This [~~paragraph~~] section shall not apply to images or videos of the depicted person made:

[~~(A)~~] (a) When the person was voluntarily nude in public or voluntarily engaging in sexual conduct in public; or

[~~(B)~~] (b) Pursuant to a voluntary commercial transaction.

~~[; and~~]

[~~(ii)~~] (3) Nothing in this [~~paragraph~~] section shall be construed to impose liability on a provider of "electronic communication service" or "remote computing service" as those terms are defined in section 803-41, for an image or video disclosed through the electronic communication service or remote computing service by another person.

[~~(2)~~] (4) Violation of privacy in the first degree is a class C felony. In addition to any penalties the court may impose, the court may order the destruction of any recording made in violation of this section.

[~~(3)~~] (5) Any recording or image made or disclosed in violation of this section and not destroyed pursuant to subsection [~~(2)~~] (4) shall be sealed and remain confidential.'"

Notes

[1] House Concurrent Resolution No. 225, H.D. 1, S.D. 1 (2019). https://www.capitol.hawaii.gov/session2019/bills/HCR225_SD1_.pdf.
[2] *Id.* at 2.
[3] *Id.*
[4] The agendas for, minutes of, and materials provided at each meeting can be accessed on a webpage created by the Hawaii State Legislature Webmaster. " Twenty-first Century Privacy Law Task Force" https://www.capitol.hawaii.gov/specialcommittee.aspx?comm=tfcpltf&year=2019.
[5] Meeting Minutes and Meeting Materials, August 21, 2019.
[6] Kelly McCanlies, MBS in Computer Science, is the former Director of Privacy Programs at Hawaiian Electric Company, and has multiple privacy certifications from the International Association of Privacy Professionals and other privacy organizations.
[7] Further information about each subsequent bullet-pointed item until reference to the September 26, 2019 meeting can be found on the Twenty-first Century Privacy Law Task Force webpage. Kelly McCanlies, *The State of Privacy Law.* August 21, 2019. https://www.capitol.hawaii.gov/committeefiles/special/TFCPLTF/HCR225TaskForce-Presentation-KellyMcCanlies.pdf.
[8] The General Data Protection Regulation is the comprehensive privacy law governing the European Union. It went into effect in 2018. *See Kelly McCanlies, The State of Privacy Law. August 21, 2019,* for more information.
[9] The California Consumer Privacy Act is the comprehensive privacy law governing California. *See Kelly McCanlies, The State of Privacy Law. August 21, 2019,* for more information.
[10] State Comprehensive-Privacy Law Comparison, International Association of Privacy Professions. *See* Meeting Materials, August 21, 2019.
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] Chapter 487N, Hawaii Revised Statutes.
[27] Task Force member Deputy Prosecuting Attorney Chris Van Marter provided the Task Force with background regarding, and proposed legislation that would amend, sections 803-46.6 and -46.7, Hawaii Revised Statutes. For proposed legislation, *see* Meeting Materials, September 26, 2019.
[28] Task Force member Deputy Prosecuting Attorney Chris Van Marter provided the Task Force with background regarding, and proposed legislation that would amend, sections 803-46.8, Hawaii Revised Statutes. For proposed legislation, *see* Meeting Materials, September 26, 2019
[29] Mericia Palma-Elmore, SAG-AFTRA, provided the Task Force with background information on the subject of deep fake technology. For proposed legislation, see Meeting Materials, September 26, 2019.
[30] Jael Makagon, Santa Clara County Privacy Office, provided the Task Force with a short explanation of issues regarding Internet Service Provider privacy. See Meeting Materials, September 26, 2019.
[31] Meeting Minutes, August 21, 2019, and November 26, 2019.
[32] Meeting Minutes, August 21, 2019.
[33] Sections 487N-1 and -2, Hawaii Revised Statutes.

[34] "The privacy and financial security of individuals is increasingly at risk due to the widespread collection of personal information by the private sector and government agencies. Numerous sources include personal information that forms the source material for identity thieves.

Identity theft is one of the fastest growing crimes committed throughout the United States, including Hawaii. Criminals who steal personal information, such as social security numbers, use the information to open credit card accounts, write bad checks, buy cars, and commit other financial crimes with other people's identities.

The purpose of this Act is to alleviate the growing plague of identity theft by requiring businesses and government agencies that maintain records containing resident individuals' personal information to notify an individual whenever the individual's personal information has been compromised by unauthorized disclosure." Act 135, Session Laws of Hawaii, 2006, Section 1.

[35] *See* Meeting Minutes, September 26, 2019.

[36] *See* Meeting Materials, November 26, 2019.

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] Proposed legislation, most recent version received by the Task Force on November 26, 2019.

[48] Meeting Minutes, November 15, 2019.

[49] Meeting Minutes, November 26, 2019.

[50] *See* note 36.

[51] Federal Trade Commission. *Data Brokers: A Call for Transparency and Accountability. Page iv-v. (May 2014.)*

[52] Meeting Materials, October 21, 2019.

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *See* note 10.

[60] *Id.*

[61] *Id.*

[62] CAL. CIV. CODE §1798.123.

[63] *Id.*

[64] *See* note 47.

[65] Subsection (a) authorizes the Attorney General or the Office of Consumer Protection to bring action against a business that violations Chapter 487N, Hawaii Revised Statutes.

[66] Section 487N-3(b), Hawaii Revised Statutes.

[67] *See* note 10.

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *Id.*
[76] *Spokeo Inc. v. Robins*, 136 S. Ct. 1540, 2016.
[77] Meeting Materials, November 15, 2019.
[78] *Id.*
[79] Section 803-46.7, Hawaii Revised Statutes.
[80] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
[81] *See* note 47.
[82] Section 803-47.8, Hawaii Revised Statutes.
[83] *See* note 35.
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *See* note 47.
[88] Facebook uses facial recognition technology to tag users in pictures.
[89] Apple iPhone models including and after the Apple iPhoneX have facial recognition technology built in as a security feature.
[90] Alfred Ng, CNET, "With facial recognition, shoplifting may get you banned in places you've never been." March 20, 2019. https://www.cnet.com/news/with-facial-recognition-shoplifting-may-get-you-banned-in-places-youve-never-been/.
[91] American Civil Liberties Union presentation, *see* Meeting Materials, October 21, 2019.
[92] *Id.*
[93] *Id.*
[94] The only county police department for which the Task Force reviewed the facial recognition technology guidelines for was the Honolulu Police Department.
[95] Honolulu Police Department Policy, Auxiliary and Technical Services, Facial Recognition Program. September 14, 2015. http://www.honolulupd.org/information/pdfs/FacialRecognitionProgram-02-04-2016-12-19-14.pdf.
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] California Assembly Bill 1215 (2019)
[105] *Id.*
[106] *Id.*
[107] *See* note 5.
[108] *Id.*
[109] *See* note 90.
[110] *Id.*
[111] *Id.*
[112] Meeting Minutes, October 21, 2019.
[113] Documents send to Task Force members via email on October 21 and 23, 2019.
[114] *See* note 35.
[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] Ryan Browne, CNBC, "Anti-election meddling group makes A.I.-powered Trump impersonator to warn about 'deepfakes.'" December 7, 2018. https://www.cnbc.com/2018/12/07/deepfake-ai-trump-impersonator-highlights-election-fake-news-threat.html.

[119] Drew Harwell, Washington Post, "Faked Pelosi videos, slowed to make her appear drunk, spread across social media." May 24, 2019. https://www.washingtonpost.com/technology/2019/05/23/faked-pelosi-videos-slowed-make-her-appear-drunk-spread-across-social-media/.
[120] Assembly Bill No. 730, 2019.
[121] *Id.*
[122] *See* note 47.
[123] Meeting Minutes and Materials, November 15, 2019.
[124] *Id.*
[125] *See* note 36.
[126] Stuart A. Thompson and Charlie Warzel, The New York Times, "How to Track President Trump." December 20, 2019. https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html.
[127] *See* note 77.
[128] *Id.*
[129] *Id.*
[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *Id.*
[135] *See* note 47.
[136] *See* note 10.
[137] *See* note 122.
[138] *See* note 77.
[139] *Id.*
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.*
[144] *See* note 10.
[145] *See* note 47.
[146] *See* note 36.
[147] *Id.*
[148] Alex Johnson, NBC News, "Trump Signs Measure to Let ISPs Sell Your Data Without Consent." April 3, 2017. https://www.nbcnews.com/news/us-news/trump-signs-measure-let-isps-sell-your-data-without-consent-n742316.
[149] *See* note 36.
[150] *Id.*
[151] *Id.*
[152] *Id.*
[153] *See* note 10.
[154] *Id.*
[155] *Id.*
[156] *Id.*
[157] *Id.*
[158] *Id.*
[159] *Id.*
[160] *Id.*
[161] *Id.*