Policy :: Information Security Laws & Regulations

Follow the links below to learn more about how federal and state laws impact information security and the use of computers.

Breach Notification Laws

Notification of Disclosure of Private Data
http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html [1]

California General Security Standard for Businesses CA AB 1950 [Released: Release 1]
http://info.sen.ca.gov/pub/03-04/bill/asm/ab_1901-1950/ab_1950_bill_20040929_chaptered.pdf [2]

SB 20 - California OPP Recommended Practices on Notification of Security Breach [Released: Release 1]
http://info.sen.ca.gov/pub/09-10/bill/sen/sb_0001-0050/sb_20_bill_20081201_introduced.html [3]

Security Breach Notice - Civil Code sections 1798.29 [4], 1798.82, and 1798.84 [5]. This law requires a business or a State agency that maintains unencrypted computerized data that includes personal information, as defined, to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The type of information that triggers the notice requirement is an individual's name plus one or more of the following: Social Security number, driver [6]'s license or California Identification Card number, financial account numbers, medical information or health insurance information. The law's intention is to give affected individuals the opportunity to take steps to protect themselves from identity theft. See the Office of Privacy Protection's Recommended Practices [7] in relation to this law.

Data Destruction

Destruction of Customer Records - California Civil Code sections 1798.80 - 1798.81 and 1798.84 [5]. This requires businesses to shred, erase or otherwise modify the personal information in records under their control.

Healthcare Privacy

AB 211 [8] - Civil, criminal, and monteary penalties for browsing, selling, or unlawfully accepting Healthcare and Psychiatric records. This is a modification to Civil Code 56. January 2009.
http://info.sen.ca.gov/pub/07-08/bill/asm/ab_0201-0250/ab_211_bill_20080930_chaptered.pdf [8]

HITECH [9] - Provides penalties for healthcare information breaches for HIPAA covered entities. Physicians will be eligible for $40,000 to $65,000 for showing that they are meaningfully using health information technology such as through reporting of quality measures. We need to find out if we are eligible for this. If so, then appropriate security measures would need to be in place to protect us from AB 211. 2009

California Constitution, Article 1, section 1 [10]. The state Constitution gives each citizen an "inalienable right" to pursue and obtain "privacy."

Computer Misuse and Abuse: Criminal Sanctions - Penal Code section 502 [11]. In general, this section

makes it a crime to knowingly access and, without permission, use, misuse, abuse, damage, contaminate, disrupt or destroy a computer, computer system, computer network, computer service, computer data or computer program. Depending on the particular violation, this section can support a variety of fines and imprisonment in criminal actions as well as remedies recoverable in civil actions.

PCI DSS

PCI DSS https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml [12]

Credit Card or Check Payment - Civil Code sections 1725 [13] and 1747.08 [14]. Any person accepting a check in payment for most goods or services at retail is prohibited from recording a purchaser's credit card number or requiring that a credit card be shown as a condition of accepting the check (Section 1725 [13]). Any person accepting a credit card in payment for most goods or services is prohibited from writing the cardholder's personal information on forms associated with the transaction (Section 1747.08 [14]).

Credit/Debit Card Number Truncation - California Civil Code section 1747.09 [14]. No more than the last five digits of a credit card or debit card number may be printed on the customer copy of electronically printed receipts.

Credit Card "Skimmers" - Penal Code section 502.6 [11]. The knowing and willful possession or use, with the intent to defraud, of a device designed to scan or re-encode information from or to the magnetic strip of a payment card (a "skimmer") is punishable as a misdemeanor. The devices owned by the defendant and possessed or used in violation may be destroyed and various other computer equipment used to store illegally obtained data may be seized.

Eavesdropping, Spying, Unauthorized Pictures

Eavesdropping or Skimming RFID – Civil Code section 1798.79 and following [15]. This law makes it a misdemeanor to intentionally remotely read or attempt to read another person’s identification document that uses radio frequency identification (RFID), without the person’s knowledge or consent. It also makes it a misdemeanor to reveal the operational system keys used in a contactless identification document. Both crimes are punishable by a jail term of up to one year and/or a fine of up to $1,500.

Electronic Eavesdropping - Penal Code sections 630-638 [16]. Among other things, this law prohibits, with exceptions, electronic eavesdropping on or recording of private communications by telephone, radio telephone, cellular radio telephone, cable or any other device or in any other manner. Violation can result in penalties of up to $10,000 and imprisonment in county jail or state prison for up to one year (sections 631-632.7). It prohibits cable TV and satellite TV operators from monitoring or recording conversations in a subscriber's residence, or from sharing individually identifiable information on subscriber viewing habits or other personal information without written consent (section 637.5).

Electronic Eavesdropping by State Law Enforcement Officials – Penal Code sections 629.50-629.98 [17]. With the approval of a Superior Court judge, specified law enforcement officials can intercept specifically described wire, electronic pager, or electronic cellular telephone communications. The law prescribes a procedure that requires officials to present to a Superior Court judge requests for authority to record, catalogue, maintain and report about recordings of all communications intercepted (except legally privileged communications). The law also requires authorities to notify the parties to such intercepted communications about the facts of the wiretapping activities, no later than 90 days after the termination of the activities or after the denial of an application seeking wiretapping authority. This law will expire on January 1, 2012.

Telecommunications Customer Privacy - Public Utilities Code sections 2891-2894.10 [18]. This law bars

telecommunications companies from disclosing the calling patterns, personal financial information or other specified personal information of residential subscribers without first getting written consent of the subscriber. There are some exceptions, including disclosure for the purpose of debt collection, for responding to a 911 call, and as required by legal process. It also requires, among other things, that telephone companies must give annual notice to subscribers that calling an 800 or 900 number may result in the disclosure of the subscriber's telephone number to the called party.

Telephone Record "Pretexting" - Penal Code section 638 [16] This law prohibits the purchase or sale of any telephone calling pattern record or list without the written consent of the subscriber.

Wireless Network Security - Business and Professions Code sections 22948.5-22948.7 [19]This law requires devices that include an integrated and enabled wireless access point that are manufactured on or after October 1, 2007, to include a warning that advises consumers about how to protect their personal information and mitigate unauthorized use of their Internet access, and provide other specified protection measures.

Physical & Constructive Invasions of Privacy - Civil Code section 1708.8 [13]. This law defines physical invasion of privacy in terms of trespassing in order to capture an image, sound recording or other impression in certain circumstances. It also defines constructive invasion of privacy as attempting to capture such an impression under circumstances in which the plaintiff had a reasonable expectation of privacy.

General Laws

California Constitution, Article 1, section 1 [10]. The state Constitution gives each citizen an "inalienable right" to pursue and obtain "privacy."

Computer Misuse and Abuse: Criminal Sanctions - Penal Code section 484-502 [11].9. In general, this section makes it a crime to knowingly access and, without permission, use, misuse, abuse, damage, contaminate, disrupt or destroy a computer, computer system, computer network, computer service, computer data or computer program. Depending on the particular violation, this section can support a variety of fines and imprisonment in criminal actions as well as remedies recoverable in civil actions.

"The Identity Theft and Assumption Deterrence Act of 1998" (18 U.S.C. 1028) makes identity theft a federal crime. http://www.ftc.gov/os/statutes/itada/itadact.htm [20]

Locking Mail Boxes in Residential Hotels – Civil Code section 1941.1 [21] and Health & Safety Code section 17958.3. Effective July 1, 2008, all residential hotels must provide each residential unit with a locking mail receptacle, acceptable for mail delivery by the U.S. Postal Service. Failure to comply is a basis for considering a residential unit un-tenantable. The law also authorizes cities and counties to make and enforce ordinances that provide greater protections and penalties.

Public Records Act - Government Code sections 6250-6268 [22]. This law applies to state and local government. It gives members of the public a right to obtain certain described kinds of documents that are not protected from disclosure by the Constitution and other laws. This law also provides some specific privacy protections.

Public Record Exemption for Sex Offense Victims - Government Code section 6254 [23] and Penal Code section 293 [24]. These laws prohibit the disclosure of the names and addresses of victims of specific sex-related crimes in documents provided in response to requests for records, including responses provided under the California Public Records Act.

Employment of Offenders - Penal Code section 4017.1 [25] and Penal Code section 5071 [26] and Welfare and Institutions Code section 219.5 [27]. Prison and county jail inmates may not have jobs that

give them access to personal information. The same prohibitions apply to offenders performing community service in lieu of a fine or custody.

Federal Education Rights and Privacy Act (FERPA [28])
- http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html [29]

California Penal Code 502 [30] - The complete text of the Penal Code of the State of California, Sections 502 and 502.01, which details the scope of computer crime and its penalties. It describes the protection afforded to individuals, businesses, and governmental agencies against tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.

“Wayne Shredding Bill” (State Civil Code 1798.80-82) –requires that sensitive information be unreadable before disposing of either electronic or paper documents.
http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84 [5]

Security of Personal Information - Civil Code section 1798.81.5 [5]. This law requires specified businesses to use safeguards to ensure the security of Californians’ personal information (defined as name plus SSN, driver’s license/state ID, financial account number) and to contractually require third parties to do the same. It does not apply to businesses that are subject to certain other information security laws.

Related Topics

Policy [31], Security [32]

Source URL: http://www.humboldt.edu/its/security-lawsandpolicies

Links:
[1] http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html
[2] http://info.sen.ca.gov/pub/03-04/bill/asm/ab_1901-1950/ab_1950_bill_20040929_chaptered.pdf
[3] http://info.sen.ca.gov/pub/09-10/bill/sen/sb_0001-0050/sb_20_bill_20081201_introduced.html
[4] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29
[5] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84
[6] http://www.humboldt.edu/its/glossary/5#term374
[7] http://www.privacy.ca.gov/res/docs/pdf/secbreach.pdf
[8] http://info.sen.ca.gov/pub/07-08/bill/asm/ab_0201-0250/ab_211_bill_20080930_chaptered.pdf
[9] http://security.sonoma.edu/laws/hitechact.pdf
[10] http://www.leginfo.ca.gov/.const/.article_1
[11] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=484-502.9
[12] https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
[13] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1708-1725
[14] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1747-1748.7
[15] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.79-1798.795
[16] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=630-638
[17] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=6

29.50-629.98
[18] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=puc&group=02001-03000&file=2891-2894.10
[19] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22948.5-22948.7
[20] http://www.ftc.gov/os/statutes/itada/itadact.htm
[21] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1940-1954.1
[22] http://www.privacy.ca.gov/pra.htm
[23] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=06001-07000&file=6250-6270
[24] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=290-294
[25] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=03001-04000&file=4000-4030
[26] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=05001-06000&file=5050-5071
[27] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=wic&group=00001-01000&file=200-224.6
[28] http://www.humboldt.edu/its/glossary/5#term298
[29] http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
[30] http://www.techlawjournal.com/statutes/calpc502.asp
[31] http://www.humboldt.edu/its/category/quicklinks/policy
[32] http://www.humboldt.edu/its/category/quicklinks/security