PRIVACY LAWS THAT IMPACT SDSU

This is a partial list of privacy laws, both State and Federal, that are pertinent to all members of the San Diego State University community. It is provided as a resource that might prove useful to faculty, staff, and students and is not intended to be a definitive source for all laws pertaining to privacy or privacy-related issues.

California State Privacy Laws

- **Credit/Debit Card Number Truncation** – California Civil Code section 1747.09. 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.

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

- **Information Practices Act of 1977** – California Civil Code 1798 and following. This law applies to state government. It expands upon the constitutional guarantee of privacy by providing limits on collection, management and dissemination of personal information by state agencies.

- **Library, Records, Confidentiality**- Government Code sections 6254,6267,6276.28. Registration and curriculum records, of libraries supported by public funds, are confidential and are explicitly exempted from the Public Records Act.

- **Public Records Act**- Government Code sections 6250-6268. This applies to state and local governments. 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.

- **Security Breach Notice**- Civil Code sections 1798.29,1798.82 and 1798.84. 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. This type of information that triggers the notice requirement is an individual’s name plus one or more of the following: Social Security number, driver’s license or state ID card number, or financial account numbers. 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 in relation to this law.

- **Social Security Number Confidentiality**- Civil Code sections 1798.85-1798.86, 1785.11.1 and 1785.11.6. This law restricts businesses and state and local agencies from publicly posting or displaying Social Security numbers. It also bans embedding SSNs on a card or document using a bar code, chip, magnetic strip or other technology, in place of removing the number as required by law. The law takes effect gradually, from 2002 through 2007. See the Office of Privacy Protection’s Recommended Practices in relation to this law.
• Medical Information Confidentiality – Civil Code section 56-56.37. This law puts limits on the disclosure of patients' medical information by medical providers, health plans, and pharmaceutical companies. It specifically prohibits many types of marketing uses and disclosures by health care providers and plans.

• Patient Access to Health Records – Health & Safety Code section 123110 and following. With minor limitations, this law gives patients the right to see and copy information maintained by health care providers relating to the patients’ health conditions. This law also gives patients the right to submit amendments to their records, if the patients believe that the records are inaccurate or incomplete.

• Computer Spyware – Business and Professions Code section 22947 and following. This law prohibits an unauthorized person from knowingly installing or providing software that performs certain functions, such as taking control of the computer or collecting personally identifiable information, on or to another computer located in California.

• Spam Laws – Business and Professions Code sections 17529 and following and 17538.45. These laws regulate “spam” unsolicited commercial e-mail. Section 17529.5 concerns unsolicited commercial e-mails with misleading or falsified headers or information, and includes penalties. It applies to e-mail sent to or from California e-mail address. It authorizes the recipient, an e-mail service provider, or the Attorney General to bring an action for actual damages and liquidated damages of $4,000 per e-mail ad sent in violation, up to $1 million per incident. It also authorizes attorney’s fees and costs to a prevailing plaintiff. Section 17538.45 gives an e-mail service provider the right to sue those who send spam from its network or to its subscribers. Service providers can get civil damages up to $25,000 per day plus attorney fees. See also the federal CAN-SPAM Act.

• Comprehensive Computer Data Access and Fraud Act – Penal code 502.C. This law expands the protection to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to computer data and systems.

Federal Privacy Laws

• Financial Services Modernization Act, Gramm-Leach-Bliley (GLB), Privacy Rule-15 U.S. Code sections 6801-6809. The 1999 federal law permits the consolidation of financial services companies and requires financial institution to issue privacy notices to their customers, giving them the opportunity to opt-out of some sharing of personally identifiable financial information with outside companies. For more information, see www.ftc.gov/privacy/privacyinitiatives/blbact.html.

• Health Insurance Portability and Accountability Act of 1996 (HIPAA) – 45 CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information and Security Standards for the Protection of Electronic Protected Health Information. HIPAA includes provisions designed to save money for health care businesses by encouraging electronic transactions and also regulations to protect the
PRIVACY LAWS THAT IMPACT SDSU

security and confidentiality of patient information. The privacy rule took effect on April 14, 2001, with most covered entities (health plans, health care clearinghouse and health care providers who conduct certain financial and administrative transactions electronically) having until April 2003 to comply. The security rule took effect on April 21, 2003. For more information, see the Web site of the federal Office of Civil Rights [http://www.hhs.gov/ocr/hipaa/](http://www.hhs.gov/ocr/hipaa/).

- **Computer Fraud and Abuse Act of 1984 – 18 U.S. Code section 1030.** This law makes unauthorized access to “Protected computers” illegal. Protected computers include U.S. government computers, computers used in interstate commerce and computers used by financial institutions. It also prohibits trafficking in computer passwords and damaging a protected computer.

- **CAN-SPAM Act of 2003 – 15 U.S. Code sections 7701-7713.** The Controlling the Assault of Non-Solicited Pornography and Marketing Act requires unsolicited commercial e-mailing messages to be labeled (though not by a standard method) and to include opt-out instructions and the sender’s physical address. It prohibits the use of deceptive subject lines and false headers in such messages. The FTC is authorized (but not required) to establish a “do-not-email” registry. The CAN-SPAM Act took effect on January 1, 2004.

- **Amendments to the Federal Rules of Civil Procedure.** The amendments took effect December 1, 2006. The new rules of procedure require consideration of the manner to preserve, maintain, and provide Electronically Stored Information (ESI) for a federal case. It mandates litigants include copies, descriptions, and locations of ESI. May induce more specific requirements on the litigants.