12-1-2011

Privacy Law Guide

Ed Rinderle
Georgia State University College of Law

Georgia State University | COLLEGE OF LAW

Research Guides

Privacy Law Guide

Guide Information

Last Updated: Jan 24, 2012
Guide URL: http://libguides.law.gsu.edu/privacylaw
Description: description - follow directions for what goes here.
Tags: advanced_legal_research
RSS: Subscribe to Updates via RSS

Guide Index

Home

Introduction

The topic of privacy and data security is a new and evolving area of the law that deals with the protection of individuals' confidential information. There are a number of areas of law that have to do with data security and privacy, and a growing number of laws of have been passed which, in part, deal with the protection of confidential information. Some of the more well known acts include: HIPPA which concerns privacy of health care records, the Fair and Accurate Credit Transaction Act (FACTA) which concerns credit reporting information, the Childern's Online Privacy Protection Act (COPPA) which deals with the online collection of personal information from children under 13 years of age, and the Gramm-Leach-Bliley Act which requires financial institutions to safeguard customers' sensitive data. In general, the subject of data privacy is broad, and contemplated in a number of places in the law.

Perhaps one of the most publicized topics of privacy and data security in the current environment regards the loss of customer information from companies. Open the Wall Street Journal or other papers and you very possibly will see an article dealing with a business that has either lost, or had stolen, some elements of what would be perceived confidential information. For example: Sony Entertainment (loss of over 100 million customer credit card numbers), T.J. Maxx (45 million credit and debit card numbers stolen), CardSystems Data (loss of 40 million credit and debit card numbers), and AT&T (security hole that exposed the email addresses of 100,000 iPad owners) are just a few of the data breaches that have occurred recently.

This research guide is iintended to be used as a resource for the field of information and data security law. In particular, the guide focuses on state laws, and possible federal legislation, that deal with the identification of personally identifiable information (PII), safeguards that need to be taken to protect this information, notification to the proper agencies and authorities if there is a breach of this information, and penalties associated with such breaches.

Further, this guide also contains resources pertaining to the field of Payment Card Industry (PCI) compliance. PCI is a data security standard created by the PCI counsel, and applies to all entities that accept electronic form of payment, such as credit cards and debit cards, for transactions. Although not government imposed, PCI compliance requires adhering to standards for the handling, storing, and processing of these electronic forms of payment, and further imposes penalties if a merchant is found to be out of compliance.

About the Author

Ed Rinderle is a student at the Georgia State University School of Law, and will be graduating in December, 2011. Mr. Rinderle currently works in the Information Technology department of a large, privately held hospitality company based in Atlanta, Georgia. Being involved in the world of I.T. and working in a corporate environment have given Mr. Rinderle broad experience in dealing with business issues regarding PCI compliance and privacy and data security, the focus of this research guide. Mr. Rinderle holds an undergraduate degree in chemical engineering, received from Clemson University in 1996.

Disclaimer

Bibliographies on this Web site were prepared for educational purposes by law students as part of Nancy P. Johnson's Advanced Legal Research course. The Law Library does not guarantee the accuracy, completeness, or usefulness of any information provided. Thorough legal research requires a researcher to update materials from date of publication; please note the semester and year the bibliography was prepared.

Back to Top

Primary Sources

Federal Bills and Statutes

Overall Summary:
Currently, there is no federal statute identifying what constitutes personally identifiable information, standards that must be followed when handling personally identifiable information, what constitutes a security breach, notification processes that must be followed if a breach occurs, remedial measures that must be occur upon breach, or penalties and fines associated with a violation or breach.

Federal legislation continues to circulate both the House of Representatives and Senate that covers these subjects, however to date, no federal legislation has been passed that creates a data security and privacy standard. The current bills in Congress are as follows:

Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011).
Synopsis: A bill to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

Latest Action: September 22, 2011 Placed on Senate Legislative Calendar under General Orders.

Sponsors and Cosponsors:
Sen. Patrick Leahy (D-VT) - Sponsor
Sen. Charles Schumer (D-NY) - Cosponsor
Sen. Benjamin Cardin (D-MD) - Cosponsor
Sen. Al Franken (D-MN) - Cosponsor
Sen. Richard Blumenthal (D-CT) - Cosponsor

Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. (2011).
Synopsis: To protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a security breach.

Latest Action: June 15, 2011 Referred to Senate committee. Status: Read twice and referred to the Committee on Commerce, Science, and Transportation.

Sponsors and Cosponsors:
Sen. Mark Pryor (D-AR) - Sponsor
Sen. John Rockefeller (D-WV) - Cosponsor

Data Breach Notification Act of 2011, S. 1408, 112th Cong. (2011).
Synopsis: To require Federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information.

Latest Action: September 22, 2011 Senate committee/subcommittee actions. Status: Committee on the Judiciary. Ordered to be reported with an amendment in the nature of a substitute favorably.

Sponsors and Cosponsors:
Sen. Dianne Feinstein (D-CA) - Sponsor

Personal Data Protection and Breach Accountability Act of 2011, S. 1535, 112th Cong. (2011).
Synopsis: To protect consumers by mitigating the vulnerability of personally identifiable information to theft through a security breach, providing notice and remedies to consumers in the wake of such a breach, holding companies accountable for preventable breaches, facilitating the sharing of post-breach technical information between companies, and enhancing criminal and civil penalties and other protections against the lunauthorized collection or use of personally identifiable information.

Latest Action: September 22, 2011 Placed on Senate legislative Calendar under General Orders.

Sponsors and Cosponsors:
Sen. Richard Blumenthal (D-CT) - Sponsor
Sen. Al Franken (D-MN) - Cosponsor

SAFE Data Act, H.R. 2577, 112th Cong. (2011).
Synopsis: To protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a security breach.

Latest Action: July 29, 2011 Referred to House subcommittee. Status: Referred to the Subcommittee on Commerce, Manufacturing, and Trade.

Sponsors and Cosponsors:
Rep. Mary Bono Mack (R-CA) - Sponsor

State Privacy Law Statutes

Overall Summary:
Forty-six states and the District of Columbia have passed statutes that create privacy and information data security standards, leaving only four states that have yet to deal with the subject (Alabama, Kentucky, New Mexico, and South Dakota). The statutes tend to cover the following topics, although the standards created by each state vary dramatically:

- What data elements constitute personally identifiable information (PII)
- Security standards that must be met for handling and storing PII
- What constitutes a security breach
- Actions that must be taken upon learning of a breach, including notification standards
- Penalties and remedial actions

ALASKA

- Alaska Stat. § 45.48.010 (2008): Disclosure of breach of security
- Alaska Stat. § 45.48.020 (2008): Allowable delay in notification
- Alaska Stat. § 45.48.030 (2008): Methods of notice
- Alaska Stat. § 45.48.040 (2008): Notification of certain other agencies
- Alaska Stat. § 45.48.050 (2008): Exception for employees and agents
- Alaska Stat. § 45.48.060 (2008): Waivers
- Alaska Stat. § 45.48.070 (2008): Treatment of certain breaches
- Alaska Stat. § 45.48.080 (2008): Violations
- Alaska Stat. § 45.48.090 (2008): Definitions

ARIZONA

- Arizona Rev. Stat. Ann. § 44-7501 (2007): Notification of breach of security system; civil penalty; preemption; exception; definitions

ARKANSAS

- Ark. Code Ann. § 4-110-101 (2005): Short title
- Ark. Code Ann. § 4-110-102 (2005): Findings and purpose
- Ark. Code Ann. § 4-110-103 (2005): Definitions
- Ark. Code Ann. § 4-110-104 (2005): Protection of personal information
- Ark. Code Ann. § 4-110-105 (2005): Disclosure of security breaches
- Ark. Code Ann. § 4-110-106 (2005): Exemptions
- Ark. Code Ann. § 4-110-107 (2005): Waiver
- Ark. Code Ann. § 4-110-108 (2005): Penalties

CALIFORNIA

- Cal. Code § 1798.81 (2003): Disposal of customer information
- Cal. Code § 1798.81.5 (2003): Reasonable security measures
- Cal. Code § 1798.82 (2003): Disclosure of security breaches
- Cal. Code § 1798.83 (2003): Disclosure to third parties for marketing or other purposes
- Cal. Code § 1798.84 (2003): Penalties

COLORADO

- Colo. Rev. Stat. § 6-1-716 (2006): Notification of security breach

CONNECTICUT

- Conn. Gen. Stat. § 36a-701(b) (2011): Breach of security re computerized data containing personal information. Disclosure of breach. Delay for criminal investigation. Means of notice. Unfair trade practice.

DELAWARE

- Del. Code. Ann. tit. 6, § 12B-101 (2005): Definitions
- Del. Code. Ann. tit. 6, § 12B-102 (2005): Disclosure of breach of security of computerized personal information by an individual or commercial entity
- Del. Code. Ann. tit. 6, § 12B-103 (2005): Procedures deemed in compliance with security breach requirements
- Del. Code. Ann. tit. 6, § 12B-104 (2005): Violations

DISTRICT OF COLUMBIA

- D.C. Code § 28-3851 (2011): Definitions
- D.C. Code § 28-3852 (2011): Notification of security breach
- D.C. Code § 28-3853 (2011): Enforcement

FLORIDA

- Fla. Stat. § 817.5681 (2005): Breach of security concerning confidential personal information in third-party possession; administrative penalties

GEORGIA

- O.C.G.A § 10-1-910 (2010): Legislative findings
- O.C.G.A § 10-1-911 (2010): Definitions
- O.C.G.A § 10-1-912 (2010): Notice of breach of security
- O.C.G.A § 10-1-913 (2010): Definitions for security freezes on consumer credit reports
- O.C.G.A § 10-1-914 (2010): Security freezes on consumer credit reports
- O.C.G.A § 10-1-915 (2010): Notice of right to obtain a security freeze on consumer credit report

HAWAII

- Haw. Rev. Stat. § 487N-2 (2008): Notice of security breach

IDAHO

- Id. Code § 28-51-103 (2006): Payment card receipts
- Id. Code § 28-51-104 (2006): Definitions
- Id. Code § 28-51-105 (2006): Disclosure of breach of security of computerized personal information by an agency, individual or a commercial entity
- Id. Code § 28-51-106 (2006): Procedures deemed in compliance with security breach requirements
- Id. Code § 28-51-107 (2006): Violations

ILLINOIS

- 815 Ill. Comp. Stat. 530/1 (2006):

INDIANA

- Ind. Code § 24-4.9-1 (2006): Application
- Ind. Code § 24-4.9-2 (2006): Definitions
- Ind. Code § 24-4.9-3 (2006): Disclosure and Notification Requirements
- Ind. Code § 24-4.9-4 (2006): Enforcement
- Ind. Code § 24-4.9-5 (2006): Preemption

IOWA

- Iowa Code § 715C.1 (2008): Definitions
- Iowa Code § 715C.2 (2008): Remedies

KANSAS

- Kan. Stat. § 50-7a01 (2009): Consumer Information; security breach; definitions
- Kan. Stat. § 50-7a02 (2009): Security breach requirements

LOUISIANA

- La. Rev. Stat. § 51:3071 (2005): Short Title
- La. Rev. Stat. § 51:3072 (2005): Legislative Findings
- La. Rev. Stat. § 51:3073 (2005): Definitions
- La. Rev. Stat. § 51:3074 (2005): Disclosure upon breach in the security of personal information; notification requirements; exemption

MAINE

- Me. Rev. Stat. tit. 10, § 1346 (2005): Short Title
- Me. Rev. Stat. tit. 10, § 1347 (2005): Definitions
- Me. Rev. Stat. tit. 10, § 1347-A (2005): Release or use of personal information prohibited
- Me. Rev. Stat. tit. 10, § 1348 (2005): Security breach notice requirements
- Me. Rev. Stat. tit. 10, § 1349 (2005): Enforcement; penalties
- Me. Rev. Stat. tit. 10, § 1350-A (2005): Rules; education and compliance
- Me. Rev. Stat. tit. 10, § 1350-B (2005): Reporting of identity theft; mandatory police report and possible investigation

MARYLAND

- Md. Code. Ann. § 14-3501 (2011): Definitions
- Md. Code. Ann. § 14-3502 (2011): Protection against unauthorized access or use
- Md. Code. Ann. § 14-3503 (2011): Security procedures
- Md. Code. Ann. § 14-3504 (2011): Security breach
- Md. Code. Ann. § 14-3505 (2011): Exclusivity and preemption
- Md. Code. Ann. § 14-3506 (2011): Notification to credit reporting agencies
- Md. Code. Ann. § 14-3507 (2011): Compliance with subtitle
- Md. Code. Ann. § 14-3508 (2011): Violations; penalties

MASSACHUSETTS

- Mass. Gen. Laws ch. 93H, § 1 (2011): Definitions
- Mass. Gen. Laws ch. 93H, § 2 (2011): Regulations to safeguard personal information of commonwealth residents
- Mass. Gen. Laws ch. 93H, § 3 (2011): Duty to report known security breach or unauthorized use of personal information
- Mass. Gen. Laws ch. 93H, § 4 (2011): Delay in notice when notice would impede criminal investigation; cooperation with law enforcement
- Mass. Gen. Laws ch. 93H, § 5 (2011): Applicability of other state and federal laws
- Mass. Gen. Laws ch. 93H, § 6 (2011): Enforcement of chapter

MICHIGAN

- Mich. Comp. Laws § 445.61 (2006): Short title
- Mich. Comp. Laws § 445.63 (2006): Definitions
- Mich. Comp. Laws § 445.72 (2006): Notice of security breach; requirements
- Mich. Comp. Laws § 445.72a (2006): Destruction of data containing personal information required; violation as misdemeanor; fine; compliance; "destroy" defined

MINNESOTA

- Minn. Stat. § 325E.61 (2006): Data warehouses; notice required for certain disclosures
- Minn. Stat. § 325E.61 (2007): Access devices; breach of security

MISSISSIPPI

- Miss. Code. Ann. § 75-24-29 (2011): Persons conducting business in Mississippi required to provide notice of a breach of security involving personal information to all affected individuals; enforcement

MISSOURI

- Mo. Rev. Stat. § 407.1500 (2010): Definitions--notice to consumer for breach of security, procedure--attorney general may bring action for damages

MONTANA

- Mont. Code. Ann. § 30-14-1701 (2007): Purpose
- Mont. Code. Ann. § 30-14-1702 (2007): Definitions
- Mont. Code. Ann. § 30-14-1703 (2005): Record destruction
- Mont. Code. Ann. § 30-14-1704 (2007): Computer security breach
- Mont. Code. Ann. § 30-14-1705 (2005): Department to restrain unlawful acts -- penalty
- Mont. Code. Ann. § 2-6-504 (2009): Notification of breach of security data system

NEBRASKA

- Neb. Rev. Stat. § 87-801 (2006): Act, how cited
- Neb. Rev. Stat. § 87-802 (2006): Terms, defined
- Neb. Rev. Stat. § 87-803 (2006): Breach of security; investigation; notice to resident
- Neb. Rev. Stat. § 87-804 (2006): Compliance with notice requirements; manner
- Neb. Rev. Stat. § 87-805 (2006): Waiver; void and unenforceable
- Neb. Rev. Stat. § 87-806 (2006): Attorney General; powers

- Neb. Rev. Stat. § 87-807 (2006): Act; applicability

NEVADA

- Nev. Rev. Stat. § 603A.010 (2005): Definitions
- Nev. Rev. Stat. § 603A.020 (2005): "Breach of the security of the system data" defined
- Nev. Rev. Stat. § 603A.030 (2005): "Data collector" defined
- Nev. Rev. Stat. § 603A.040 (2007): "Personal information" defined
- Nev. Rev. Stat. § 603A.100 (2005): Waiver of provisions of chapter prohibited
- Nev. Rev. Stat. § 603A.200 (2005): Destruction of certain records
- Nev. Rev. Stat. § 603A.210 (2005): Security measures
- Nev. Rev. Stat. § 603A.215 (2009): Security measures for data collector that accepts payment card; use of encryption; liability for damages; applicability
- Nev. Rev. Stat. § 603A.220 (2005): Disclosure of breach of security of system data; methods of disclosure
- Nev. Rev. Stat. § 603A.900 (2005): Civil action
- Nev. Rev. Stat. § 603A.910 (2005): Restitution
- Nev. Rev. Stat. § 603A.920 (2005): Injunction

NEW HAMPSHIRE

- N.H. Rev. Stat. Ann. § 359-C:19 (2006): Definitions
- N.H. Rev. Stat. Ann. § 359-C:20 (2006): Notification of Security Breach Required
- N.H. Rev. Stat. Ann. § 359-C:21 (2006): Violation

NEW JERSEY

- N.J. Rev. Stat. § 56:8-161 (2005): Definitions relative to security of personal information
- N.J. Rev. Stat. § 56:8-162 (2005): Methods of destruction of certain customer records
- N.J. Rev. Stat. § 56:8-163 (2005): Disclosure of breach of security to customers
- N.J. Rev. Stat. § 56:8-164 (2005): Prohibited actions relative to display of social security numbers

NEW YORK

- N.Y. Gen. Bus. L. § 899-aa (2011): Notification; person without valid authorization has acquired private information

NORTH CAROLINA

- N.C. Gen. Stat. § 75-65 (2009): Protection from security breaches

NORTH DAKOTA

- N.D. Cent. Code § 51-30-01 (2011): Definitions
- N.D. Cent. Code § 51-30-02 (2011): Notice to consumers
- N.D. Cent. Code § 51-30-03 (2011): Notice to owner or licensee of personal information
- N.D. Cent. Code § 51-30-04 (2011): Delayed notice
- N.D. Cent. Code § 51-30-05 (2011): Method of notice
- N.D. Cent. Code § 51-30-06 (2011): Alternate compliance
- N.D. Cent. Code § 51-30-07 (2011): Enforcement - Powers - Remedies - Penalties

OHIO

- Ohio Rev. Code Ann. § 1347.12 (2007): Agency disclosure of security breach of computerized personal information data
- Ohio Rev. Code Ann. § 1349.19 (2007): Private disclosure of security breach of computerized personal information data
- Ohio Rev. Code Ann. § 1349.191 (2006): Investigation of noncompliance with disclosure laws
- Ohio Rev. Code Ann. § 1349.192 (2006): Civil action by attorney general for violation of disclosure laws

OKLAHOMA

- Okla. Stat. § 74-3113.1 (2011): Disclosure of information indexed by social security numbers prohibited - Exceptions
- Okla. Stat. § 24-161 (2008): Short title

- Okla. Stat. § 24-162 (2008): Definitions
- Okla. Stat. § 24-163 (2008): Duty to disclose breach
- Okla. Stat. § 24-164 (2008): Notice procedures deemed in compliance
- Okla. Stat. § 24-165 (2008): Enforcement - Civil penalty limitation
- Okla. Stat. § 24-166 (2008): Application of act

OREGON

- Or. Rev. Stat. § 646A.600 (2009): Short title
- Or. Rev. Stat. § 646A.600 (2009): Definitions
- Or. Rev. Stat. § 646A.600 (2009): Notice of breach of security; delay; methods of notification; contents of notice; application of notice requirement

PENNSYLVANIA

- 73 Pa. Stat. § 2301 (2005): Short title
- 73 Pa. Stat. § 2302 (2005): Definitions
- 73 Pa. Stat. § 2303 (2005): Notification of breach
- 73 Pa. Stat. § 2304 (2005): Exceptions
- 73 Pa. Stat. § 2305 (2005): Notification of consumer reporting agencies
- 73 Pa. Stat. § 2306 (2005): Preemption
- 73 Pa. Stat. § 2307 (2005): Notice of exemption
- 73 Pa. Stat. § 2308 (2005): Civil relief
- 73 Pa. Stat. § 2329 (2005): Applicability

RHODE ISLAND

- R.I. Gen. Laws § 11-49.2-1 (2005): Short title
- R.I. Gen. Laws § 11-49.2-2 (2005): Legislative findings
- R.I. Gen. Laws § 11-49.2-3 (2005): Notification of breach
- R.I. Gen. Laws § 11-49.2-4 (2005): Notification of breach - Consultation with law enforcement
- R.I. Gen. Laws § 11-49.2-5 (2005): Definitions
- R.I. Gen. Laws § 11-49.2-6 (2005): Penalties for violation
- R.I. Gen. Laws § 11-49.2-7 (2005): Agencies with security breach procedures

SOUTH CAROLINA

- S.C. Code § 39-1-90 (2010): Breach of security business data; notification; definitions; penalties; exception as to certain banks and financial institutions; notice to Consumer Protection Division
- S.C. Code § 37-20-110 (2010): Definitions
- S.C. Code § 37-20-150 (2010): Records of individuals who have been victims of identity theft to be maintained by State law Enforcement Division; submission of fingerprints and other required information by victims
- S.C. Code § 37-20-190 (2010): Requirements for disposition of business records; exceptions

TENNESSEE

- Tenn. Code § 47-18-2107 (2011): Release of personal consumer information
- Tenn. Code § 49-7-216 (2011): Confidential data or records of students enrolled in TICUA institutions

TEXAS

- Tex. Bus. & Com. Code § 521.002 (2009): Definitions
- Tex. Bus. & Com. Code § 521.051 (2009): Unauthorized use or possession of personal identifying information
- Tex. Bus. & Com. Code § 521.052 (2009): Business duty to protect sensitive personal information
- Tex. Bus. & Com. Code § 521.053 (2009): Notification required following breach of security or computerized data

UTAH

- Utah Code § 13-44-101 (2011): Title

- Utah Code § 13-44-102 (2011): Definitions
- Utah Code § 13-44-201 (2011): Protection of personal information
- Utah Code § 13-44-202 (2011): Personal information - Disclosure of system breaches
- Utah Code § 13-44-301 (2011): Enforcement

VERMONT

- Vt. Stat. tit. 9, § 2430 (2005): Definitions
- Vt. Stat. tit. 9, § 2435 (2005): Notice of security breaches
- Vt. Stat. tit. 9, § 2440 (2005): Social security number protection
- Vt. Stat. tit. 9, § 2440 (2005): Safe destruction of documents containing personal information

VIRGINIA

- Va. Code § 18.2-186.6 (2008): Breach of personal information notification
- Va. Code § 32.1-127.1:05 (2010): Breach of medical information notification

WASHINGTON

- Wash. Rev. Code § 19.255.010 (2005): Disclosure, notice - Definitions - Rights, remedies
- Wash. Rev. Code § 42.56.590 (2007): Personal information - Notice of security breaches

WEST VIRGINIA

- W. Va. Code § 46A-2A-101 (2011): Definitions
- W. Va. Code § 46A-2A-102 (2011): Notice of breach of security of computerized personal information
- W. Va. Code § 46A-2A-103 (2011): Procedures deemed in compliance with security breach notice requirements
- W. Va. Code § 46A-2A-104 (2011): Violations
- W. Va. Code § 46A-2A-105 (2011): Applicability

WISCONSIN

- Wis. Stat. § 134.97 (2010): Disposal of records containing personal information
- Wis. Stat. § 134.98 (2010): Notice of unauthorized acquisition of personal information
- Wis. Stat. § 134.99 (2010): Parties to violation

WYOMING

- Wyo. Stat. § 40-12-501 (2011): Definitions
- Wyo. Stat. § 40-12-502 (2011): Computer security breach; notice to affected persons

Cases

Overall Summary:
Case law in the area of data security and privacy is just beginning to emerge. Of the few cases that do exist, the typical cause of action will relate to either an existing state statue, unfair trade practices claims, or general negligence claims.

In Re Hannaford Brothers, 613 F.Supp.2d 108 (D. Me. 2009).
Summary: In Hannaford, customer credit card data was stolen by a third party from the merchant, a grocer, where the customers had used their credit cards. The customers claimed that Hannaford was negligent in failing to maintain the security of "private and confidential financial and personal information." The issue in the case was whether the customer could recover from the merchant any loss resulting from the data theft. The Court concluded that "if the negligence does not produce that completed direct financial loss and instead causes only collateral consequences-for example, the customer's fear that a fraudulent transaction might happen in the future, the consumer's expenditure of time and effort to protect the account, lost opportunities to earn reward points, or incidental expenses that the customer suffers in restoring the integrity of the previous account relationships-then the merchant is not liable." The case was further dismissed for all plaintiffs, with the exception of one.

Pineda v. Williams-Sonoma Stores, Inc., 51 Cal.4th 524 (2011).
Summary: Plaintiff, Jessica Pineda, was checking out at a Williams-Sonoma retail store when the cashier requested that she provide her zip code. Believing she was required to do so, Ms. Pineda did in fact provide her zip code to the retailer. The California Supreme Court found that under the Credit Card Act, a zip code constituted "personal identification information." As a result of this finding, California businesses are effectively prohibited from collecting customer's zip code when that customer is paying for the transaction with a credit card.

Other Federal Statutes Dealing with Data Security and Privacy

Various federal statutes and regulations exist dealing with different elements of privacy and data security that are not limited to the main subject of this research guide. The three statutes below are a sampling of these broader topics.

- Gramm-Leach-Bliely Act, 15. U.S.C. § 6801 (2010).
  - Also known as the Financial Services Modernization Act of 1999, financial institutions are required to 1. Insure the security and confidentiality of customer records and information, 2. Protect against any anticipated threats or hazards to the security or integrity of such record, and 3. Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.
- Children's Online Privacy Protection Act, 15 U.S.C. § 6501-06 (2010).
  - Websites that collect information from children that are under 13 years of age must comply with COPPA
- FTC Safeguards Rule, 16 C.F.R. § 314.4 (2011).
  - The Safeguards Rule implements the security provisions of the Gramm-Leach-Bliley Act, requiring financial institutions to have in place a comprehensive security program to ensure confidentiality and security of customer data.

Back to Top

Secondary Sources

Law Journal Articles

Erika McCallister & Tim Grance & Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standards and Technology Special Publication 800-122, April 2010.

Written as guidance for U.S. Government agencies and those who conduct business on the agencies' behalf, this publication is also useful to non-governmental entities from a conceptual standpoint. The document lays out the methodology that organizations should think through in light of Personally Identifiable Information (PII), which include: Identify PII in the environment; Minimize use and storage of PII where possible; Categorize PII by impact level (risk to the organization); Apply appropriate safeguards based off of the impact level; and Develop incident response plans to handle a breach of PII. In addition, the article encourages organizations as a whole to coordinate efforts when it comes to PII related issues.

Kimberly Kiefer Peretti, *Data Breaches: What the Underground World of "Carding" Reveals*, 25 Santa Clara Computer & High Tech. L.J. 375 (2008).

Written by Senior Counsel with the United States Department of Justice's Computer Crime and Intellectual Property Sections, Ms. Peretti discusses the ways in which criminals gain access to vast amounts of stored credit and debit card data, and then the methods, called "carding forums," through which the criminals can sell the information through the internet. The note further discusses recent data breaches, and ways that the government could more effectively prosecute those responsible.

Paul M. Schwartz and Edward J. Janger, *Notification of Data Security Breaches*, 105 Mich. L. Rev. 913 (2007).

At time of writing, Mr. Schwartz was a Professor of Law at University of California Berkeley, and Mr. Janger was a Professor at Brooklyn Law School. This note reviews the data security laws of various states, and in particular the consumer notification requirements in those state statutes. The note further looks at the ramifications of breach notifications: from over notifying consumers (akin to crying wolf), to the effect that notification can serve to mitigate harm after a breach, to the reputational damage that can occur when a company must disclose a breach. The note argues for the creation of a "Coordinated Response Agent" (CRA), which would serve to promulgate information sharing of breaches, and create clearer standards and greater oversight for when consumers should be notified of data breaches.

Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. Rev. 255 (2005).

As a visiting Professor of Law at Notre Dame, Professor Johnson delves into the topic of the role of tort liability for data breaches. The note discusses the ramifications to individuals of data security theft, which can include loss of names, birth dates, social security numbers, and financial records. The note goes on to discuss theories of recovery for victims of data theft, including holding the "database possessor" liable for breaches. The note reviews database possessors' duty to safeguard individuals' data, the database possessor's legal obligation to disclose evidence of a security breach, and the extent to which the database possessor should be liable for such breach.

Joseph D. Jean and Rachel M. Wrightson, *Insurance for Information Stolen in Data Breaches*, New York Law Journal , Oct. 25, 2011.

The authors discuss the ability to file insurance claims for data breaches under general liability insurance coverage. As a case in point, the authors reference Zurich American Insurance Company v. Sony Corporation of America, in which Zurich is suing to absolve its responsibility for Sony's loss of over 100 million subscribers' credit card data due to hacker attacks. The authors conclude that upon a data breach, companies should put their general liability insurance carrier on notice, and should not accept an insurance carrier's denial of coverage as final.

Kathryn E. Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 Fordham L. Rev. 355 (2006).

Written by J.D. candidate Kathryn Picanso, this note discusses various data security breaches, and suggests a framework for legislation. In particular, the note looks at the then current (2006) data security laws at both the federal and state level, reviews alternate approaches for data security laws, and finally recommends a new framework for data security regulation.

Government Agency Security Policies

Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security, Updated Oct. 6, 2011, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf.

This handbook contains the data elements that the Department of Homeland Security considers to be sensitive personally identifiable information, and further outlines the Department's rules and policies for the handling, use, storage, and destruction of such data.

Books

Douglas E. Salane, Cyber Infrastructure Protection 51 (Tarek Saadawi and Louis Jordan, Jr. eds.) (2011).

The book as a whole covers many topics related to cybersecurity, including those that range from technical architecture, to policy. The page cited, 51, begins the chapter titled "Are Large Scale Data Breaches Inevitable?," which examines data breaches, methods that could be used to protect against such breaches (such as end-to-end encryption and continuous system patching), as well as recommended notification standards.

ALR

Jay M. Zitter, *Validity, Construction, and Application of Credit Card Number and Expiration Date Truncation Requirement, and Related Provisions, of Fair and Accurate Credit Transactions Acts (FACTA), 15 U.S.C.A. § 1681c(g), 1681n*, 51 A.L.R. Fed.2d 273 (2010).

Summary: This article discusses credit card number truncation requirements on receipts, found in the Fair and Accurate Credit Transactions Act (FACTA), and reviews court decisions regarding theses sections of FACTA, including court decisions concluding that the damages provision of FACTA is unconstitutionally vague.

Back to Top

Computerized Research, Blogs, and Twitter Feeds

Privacy and Data Security Law Blogs

Privacy Law Blogs

- Privacy Law Blog
  http://privacylaw.proskauer.com/
  Proskauer Rose LLP
  Proskauer is an international law firm with a group specializing in privacy and data security. Proskauer's Privacy Blog covers a myriad of data security topics, ranging from updates of data security laws in both the U.S. and internationally, as well as the latest cases on point.
- Privacy and Information Security Law Blog
  http://www.huntonprivacyblog.com/
  Hunton & Williams LLP
  Hunton & Williams is an international law firm that is recognized for its data and privacy practice. As well as covering domestic issues, the Hunton & Williams blog is a good and often updated resource for the latest international updates in the field of data security and privacy (not solely for new international data security laws, but also for updates to existing international laws).
- InsidePrivacy, Updates on Developments in Global Privacy & Data Security
  http://www.insideprivacy.com/
  Covington & Burling LLP
  This blog, authored by Covington & Burling, covers global privacy and data security.
- Data Privacy Monitor
  http://www.dataprivacymonitor.com/
  Baker Hostetler LLP
  This blog has a solid focus on a number of domestic data and privacy law issues, ranging from Payment Card Industry (PCI) compliance updates, to the latest cases on data breaches. In addition, the blog contains many entries that would be useful to those in corporate security and compliance.
- The Not-So Private Parts
  http://blogs.forbes.com/kashmirhill/
  By: Kashmir Hill
  Written by Kashmir Hill, who has various editorial and legal career experiences, this blog, as accurately depicted by the author, explores the intersection of privacy law with social media and technology.

Data Breach Research

- Privacy Rights Clearinghouse
  https://www.privacyrights.org/data-breach
  Privacy Rights Clearinghouse is a well constructed consumer facing website that is both educational and useful for recent consumer impacting privacy updates. The site

contains information on privacy topics including identity theft, medical privacy, social security numbers, online privacy, shopping privacy, etc.
Particularly interesting is the section on the latest data security breaches, to which the link above is directed.

- Verizon Business 2011 Data Breach Investigations Report
  http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
  An annual publication by Verizon Business, this report includes a look back at the prior year in information data security, and has useful facts such as numbers of reported breaches, industries that are targets of breaches, methods used to breach systems, countries where threat attacks originate, etc.
- Databreaches.net - Office of Inadequate Security
  http://www.databreaches.net/
  This website contains information and articles written regarding recent data breaches, and further has updates to laws being contemplated at both a federal and state level regarding information data security.

Notable Privacy and Data Security Twitter Feeds

- David Hoffman
  http://twitter.com/#!/hoffprivacy
  David Hoffman is Director of Security Policy and Global Privacy Officer at Intel Corporation, and brings good perspective from the corporate governance side of data security.
- Daniel J. Solove
  http://twitter.com/#!/DanielSolove
  Mr. Solove is a law professor at George Washington University Law School, and has in depth expertise in information privacy law.
- PrivacyMemes
  http://twitter.com/#!/PrivacyMemes
  Various privacy topics covered, including regulation, mobile, social media, case analysis, and more.
- Jon Neiditz
  http://twitter.com/#!/jonneiditz
  Jon Neiditz is an attorney practicing in Atlanta, and he covers various topics in the Information Technology and privacy realms.
- PRC_Amber
  http://twitter.com/#!/PRC_Amber
  A privacy advocate at Privacy Rights Clearinghouse, Ms. Amber Yoo tweets about a number of topics, many relating to updates and interests regarding privacy concerns and social media.

Back to Top

Payment Card Industry (PCI) Compliance

PCI Compliance Summary

Overall Summary:
If you are a merchant who accepts credit cards, then you are subject to the Payment Card Industry Data Security Standard (PCI DSS).

PCI Resources

PCI Security Standards Council

PCI
The PCI Security Standards Council creates the standards that merchants must adhere to for PCI compliance. This site contains links to documents that are required for PCI compliance, including:

- PCI Data Security Standard (PCI DSS)
- Self Assessment Questionnaires
- Pin Transaction Security (PTS)

PA-DSS
In addition, if you are a merchant using a point-of-sale system that accepts credit or debit cards as a form of payment, the application which you use must be PA-DSS (Payment Application Data Security Standard) certified. Information on PA-DSS can be found here, and a list of payment applications that are PA-DSS validated can be found here.

Security Assessments
PCI may require merchants to use Qualified Security Assessors (QSA's) to perform audits that assess a merchant's compliance with the PCI standard. A listing of QSA's can be found here, and a listing of payment application QSA's (PA-QSAs) can be found here.

Back to Top