311 Privacy, Spam, & Spyware 2006

Lael Bellamy
Director
The Home Depot

Allen Brandt
Associate Director, Privacy
Graduate Management Admission Council

Donna Lewis
Counsel
Kilpatrick Stockton LLP

Faculty Biographies

Lael Bellamy

Lael Bellamy is director-legal of Home Depot U.S.A., Inc. in Atlanta. Her responsibilities include providing legal counsel to the organization in the areas information technology, e-commerce, outsourcing, telecom and privacy.

Prior to joining The Home Depot, Ms. Bellamy was assistant vice president and senior counsel of ChoicePoint, Inc.

Ms. Bellamy received a B.S. from Cornell University and is a graduate of the Emory University School of Law.

Allen Brandt

Allen Brandt is the associate director, privacy, at the Graduate Management Admission Council (GMAC). His responsibilities include providing legal guidance to the organization primarily in the area of consumer privacy, covering both domestic and international issues. He is also involved with insuring compliance with marketing materials and corporate privacy and security matters.

Prior to joining GMAC, Mr. Brandt was the chief privacy officer and general counsel at Virtumundo, Inc., an online marketing agency, where he provided guidance in a variety of areas of CAN-SPAM and consumer privacy issues.

Mr. Brandt is a member of both the California and Missouri Bar, and has been active in ACC's Kansas City Chapter leading the volunteer effort.

Mr. Brandt is a graduate of Western State University College of Law.

Donna Lewis

Donna K. Lewis is counsel in the technology and communications section of the corporate department at Kilpatrick Stockton in Atlanta. Her focus is on the representation of (i) technology and communications companies in general corporate matters (e.g., funding, M&A, securities and commercial transactions), and (ii) companies outside of those industry sectors in commercial contracting matters focused on the use of technology to launch new businesses or revolutionize current operations (e.g., outsourcing, software licensing and procurement). In connection with those representations, she has developed specialized experience in media, convergence, open source software and data privacy and security issues.

Prior to joining Kilpatrick Stockton, Ms. Lewis spent many years at Turner Broadcasting System, Inc. in a variety of legal roles, as well as senior vice president of business development for CNN Interactive. In her most recent role as senior vice president and chief legal officer of Turner Entertainment Group, she managed the legal team responsible for representation of the Turner Entertainment Networks and related assets and was responsible for providing strategic counsel in a variety of substantive areas, including software and content licensing, intellectual property and distribution, related to the Turner's launch of digital based products and services such as broadband video, interactive television and HDTV.

She serves on the board of trustees for an Atlanta school and does pro bono work for a variety of clients in arts and entertainment.

Ms. Lewis received A.B. and M.A. from the University of Georgia and a J.D. from Emory University.

Privacy, Spam & Spyware 2006

Section 311 – ACC Annual Meeting

October 23, 2006

A Chronology of Data Breaches
Reported Since the ChoicePoint Incident

The data breaches noted below have been reported because the personal information compromised includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers. A few breaches that do NOT expose such sensitive information have been included in order to underscore the variety and frequency of data breaches. However, we have not included the number of records involved in such breaches in the total because we want this compilation to reflect breaches that expose individuals to identity theft as well as breaches that qualify for disclosure under state laws.

The running at the end of the Chronology represents the approximate number of *records* that have been compromised due to security breaches, not necessarily the number of *individuals* affected. Some individuals may be the victims of more than one breach, which would affect the totals.

This chronology below begins with ChoicePoint's 2/15/05 announcement of its data breaches because it was a watershed event in terms of disclosure to the affected individuals. Since then, the "best practice" has been to disclose breaches to individuals nationwide -- in a sense, adopting California's notice requirement nationally.

DATE MADE PUBLIC	NAME (Location)	TYPE OF BREACH	NUMBER OF RECORDS
Feb. 15, 2005	ChoicePoint (Alpharetta, GA)	Bogus accounts established by ID thieves	145,000
Feb. 25 , 2005	Bank of America (Charlotte, NC)	Lost backup tape	1,200,000
Feb. 25, 2005	PayMaxx (Miramar, FL)	Exposed online	25,000
March 8, 2005	DSW/Retail Ventures (Columbus, OH)	Hacking	100,000
March 10, 2005	LexisNexis (Dayton, OH)	Passwords compromised **UPDATE** (06.30.06): Last week, five men were arrested in connection with this breach.	32,000
March 11, 2005	Univ. of CA, Berkeley (Berkeley, CA)	Stolen laptop	98,400
March 11, 2005	Boston College (Boston, MA)	Hacking	120,000
March 12, 2005	NV Dept. of Motor Vehicle	Stolen computer, later recovered.	[8,900] Not included in total below
March 20, 2005	Northwestern Univ. (Evanston, IL)	Hacking	21,000
March 20, 2005	Univ. of NV., Las Vegas (Las Vegas, NV)	Hacking	5,000
March 22, 2005	Calif. State Univ. (Chico, CA)	Hacking	59,000
March 23, 2005	Univ. of CA. (San Francisco, CA)	Hacking	7,000
March 28, 2005	Univ. of Chicago Hospital (Chicago, IL)	Dishonest insider	Unknown
April ?, 2005	Georgia DMV	Dishonest insider	465,000
April 5, 2005	MCI (Ashburn, VA)	Stolen laptop	16,500
April 8, 2005	Eastern National	Hacker	15,000
April 8, 2005	San Jose Med. Group (San Jose, CA)	Stolen computer	185,000
April 11, 2005	Tufts University (Boston, MA)	Hacking	106,000
April 12, 2005	LexisNexis (Dayton, OH)	Passwords compromised **UPDATE** (06.30.06): Last week, five men were arrested in connection with this breach.	Additional 280,000
April 14, 2005	Polo Ralph Lauren/HSBC (New York, NY)	Hacking	180,000
April 14, 2005	Calif. Fastrack	Dishonest Insider	4,500

US2000 9491609.1

April 15, 2005	CA Dept. of Health Services	Stolen laptop	21,600
April 18, 2005	DSW/ Retail Ventures (Columbus, OH)	Hacking	Additional 1,300,000
April 20, 2005	Ameritrade (Bellevue, NE)	Lost backup tape	200,000
April 21, 2005	Carnegie Mellon Univ. (Pittsburg, PA)	Hacking	19,000
April 26, 2005	Mich. State Univ's Wharton Center	Hacking	40,000
April 26, 2005	Christus St. Joseph's Hospital (Houston, TX)	Stolen computer	19,000
April 28, 2005	Georgia Southern Univ.	Hacking	"tens of thousands"
April 28, 2005	Wachovia, Bank of America, PNC Financial Services Group and Commerce Bancorp	Dishonest insiders	676,000
April 29, 2005	Oklahoma State Univ.	Missing laptop	37,000
May 2, 2005	Time Warner (New York, NY)	Lost backup tapes	600,000
May 4, 2005	CO. Health Dept.	Stolen laptop	1,600 (families)
May 5, 2005	Purdue Univ. (West Lafayette, IN)	Hacking	11,360
May 7, 2005	Dept. of Justice (Washington, D.C.)	Stolen laptop	80,000
May 11, 2005	Stanford Univ. (Stanford, CA)	Hacking	9,900
May 12, 2005	Hinsdale Central High School (Hinsdale, IL)	Hacking	2,400
May 16, 2005	Westborough Bank (Westborough, MA)	Dishonest insider	750
May 18, 2005	Jackson Comm. College (MI)	Hacking	8,000
May 18, 2005	Univ. of Iowa	Hacking	30,000
May 19, 2005	Valdosta State Univ. (GA)	Hacking	40,000
May 26, 2005	Duke Univ. (Durham, NC)	Hacking	5,500
May 27, 2005	Cleveland State Univ. (Cleveland, OH).	Stolen laptop **Update 12/24:** CSU found the stolen laptop	[44,420] Not included in total below
May 28, 2005	Merlin Data Services (Kalispell, MT)	Bogus acct. set up	9,000
May 30, 2005	Motorola	Computers stolen	Unknown
June 6, 2005	CitiFinancial	Lost backup tapes	3,900,000
June 10, 2005	Fed. Deposit Insurance Corp. (FDIC)	Not disclosed	6,000
June 16, 2005	CardSystems	Hacking	40,000,000
June 17, 2005	Kent State Univ.	Stolen laptop	1,400
June 18, 2005	Univ. of Hawaii	Dishonest Insider	150,000
June 22, 2005	Eastman Kodak	Stolen laptop	5,800
June 22, 2005	East Carolina Univ.	Hacking	250
June 25, 2005	Univ. of CT (UCONN)	Hacking	72,000
June 28, 2005	Lucas Cty. Children Services (OH)	Exposed by email	900
June 29, 2005	Bank of America	Stolen laptop	18,000
June 30, 2005	Ohio State Univ. Med. Ctr.	Stolen laptop	15,000
July 1, 2005	Univ. of CA, San Diego	Hacking	3,300
July 6, 2005	City National Bank	Lost backup tapes	Unknown
July 7, 2005	Mich. State Univ.	Hacking	27,000

July 19, 2005	Univ. of Southern Calif. (USC)	Hacking	270,000 possibly accessed; "dozens" exposed
July 21, 2005	Univ. of Colorado-Boulder	Hacking	42,000
July 30, 2005	San Diego Co. Employees Retirement Assoc.	Hacking	33,000
July 30, 2005	Calif. State Univ., Dominguez Hills	Hacking	9,613
July 31, 2005	Cal Poly-Pomona	Hacking	31,077
Aug. 2, 2005	Univ. of Colorado	Hacking	36,000
Aug. 9, 2005	Sonoma State Univ.	Hacking	61,709
Aug. 9, 2005	Univ. of Utah	Hacking	100,000
Aug. 10, 2005	Univ. of North Texas	Hacking	39,000
Aug. 17, 2005	Calif. State University, Stanislaus	Hacking	900
Aug. 19, 2005	Univ. of Colorado	Hacking	49,000
Aug. 22, 2005	Air Force	Hacking	33,300
Aug. 27, 2005	Univ. of Florida, Health Sciences Center/ChartOne	Stolen Laptop	3,851
Aug. 30, 2005	J.P. Morgan, Dallas	Stolen Laptop	Unknown
Aug. 30, 2005	Calif. State University, Chancellor's Office	Hacking	154
Sept. 2, 2006	Iowa Student Loan(W. Des Moines)	Compact disk containing personal information, including SSNs, was lost when shipped by private courier.	165,000
Sept. 10, 2005	Kent State Univ.	Stolen computers	100,000
Sept. 15, 2005	Miami Univ.	Exposed online	21,762
Sept. 16, 2005	ChoicePoint (2nd notice, see 2/15/05 for 145,000) (Alpharetta, GA)	ID thieves accessed; also misuse of IDs & passwords.	9,903
Sept. 17, 2005	North Fork Bank, NY	Stolen laptop (7/24/05) with mortgage data	9,000
Sept. 19, 2005	Children's Health Council, San Jose CA	Stolen backup tape	5,000 - 6,000
Sept. 22, 2005	City University of New York	Exposed online	350
Sept. 23, 2005	Bank of America	Stolen laptop with info of Visa Buxx users (debit cards)	Not disclosed
Sept. 28, 2005	RBC Dain Rauscher	Illegitimate access to customer data by former employee	100+ customers' records compromised out of 300,000
Sept. 29, 2005	Univ. of Georgia	Hacking	At least 1,600
Oct. 12, 2005	Ohio State Univ. Medical Center	Exposed online. Appointment information including SSN, DOB, address, phone no., medical no., appointment reason, physician.	2,800
Oct. 15, 2005	Montclair State Univ.	Exposed online	9,100
Oct. 21, 2005	Wilcox Memorial Hospital, Hawaii	Lost backup tape	130,000
Nov. 1, 2005	Univ. of Tenn. Medical Center	Stolen laptop	3,800
Nov. 4, 2005	Keck School of Medicine, USC	Stolen computer	50,000
Nov. 5, 2005	Safeway, Hawaii	Stolen laptop	1,400 in Hawaii, perhaps more elsewhere
Nov. 8, 2005	ChoicePoint (Alpharetta, GA)	Bogus accounts established by ID thieves. Total affected now reaches 162,000 (See Feb. 15 & Sept. 16)	17,000 more
Nov. 9, 2005	TransUnion	Stolen computer	3,623
Nov. 11, 2005	Georgia Tech Ofc. of Enrollment Services	Stolen computer, Theft 10/16/05	13,000

US2000 9491609.1

Nov. 11, 2005	Scottrade Troy Group	Hacking	Unknown
Nov. 19, 2005	Boeing	Stolen laptop with HR data incl. SSNs and bank account info.	161,000
Dec. 1, 2005	Firstrust Bank	Stolen laptop	100,000
Dec. 1, 2005	Univ. of San Diego (San Diego, CA)	Hacking. Faculty, students and employee tax forms containing SSNs	7,800
Dec. 2, 2005	Cornell Univ.	Hacking. Names, addresses, SSNs, bank names and acct. numbers.	900
Dec. 6, 2005	WA Employment Security Dept.	Stolen laptop. Names, SSNs and earnings of former employees.	530
Dec. 12, 2005	Sam's Club/Wal-Mart	Exposed credit card data at gas stations.	Unknown
Dec. 16, 2005	La Salle Bank, ABN AMRO Mortgage Group	Backup tape with residential mortgage customers lost in shipment by DHL, containing SSNs and account information. **Update 12/20:** DHL found the lost tape	[2,000,000] Not included in total below.
Dec. 16, 2005	Colorado Tech. Univ.	Email erroneously sent containing names, phone numbers, email addresses, Social Security numbers and class schedules.	1,200
Dec. 20, 2005	Guidance Software, Inc.	Hacking. Customer credit card numbers	3,800
Dec. 22, 2005	Ford Motor Co.	Stolen computer. Names and SSNs of current and former employees.	70,000
Dec. 25, 2005	Iowa State Univ.	Hacking. Credit card information and Social Security numbers.	5,500
Dec. 28, 2005	Marriot International	Lost backup tape. SSNs, credit card data of time-share owners	206,000
Late Dec.	Ameriprise	Stolen laptop containing names and Social Security numbers and in some cases, Ameriprise account information.	Unknown
2005 [Exact Date Unknown]	Dept. of Veterans Affairs (Washington, D.C.)	A laptop being stored in the trunk of a car was stolen in Minneapolis, Minnesota. 2 people later reported identity fraud problems.	66
Jan. 1, 2006	University of Pittsburgh Medical Center, Squirrel Hill Family Medicine	6 Stolen computers. Names, Social Security numbers, birthdates	700
Jan. 2, 2006	H&R Block	SSNs exposed in 40-digit number string on mailing label	Unknown
Jan. 9, 2006	Atlantis Hotel - Kerzner Int'l	Dishonest insider or hacking. Names, addresses, credit card details, Social Security numbers, driver's licence numbers and/or bank account data.	55,000
Jan. 12, 2006	People's Bank	Lost computer tape containing names, addresses, Social Security numbers, and checking account numbers.	90,000
Jan. 17, 2006	City of San Diego, Water & Sewer Dept. (San Diego, CA)	Dishonest employee accessed customer account files, including SSNs, and committed identity theft on some individuals.	Unknown
Jan. 20, 2006	Univ. Place Conference Center & Hotel, Indiana Univ.	Hacking. Reservation information including credit card account number compromised.	Unknown
Jan. 21, 2006	California Army National Guard	Stolen briefcase with personal information of National Guardsmen including a "seniority roster," Social Security numbers and dates of birth.	"hundreds of officers"
Jan. 23, 2006	Univ. of Notre Dame	Hackers accessed Social Security numbers, credit card information and check images of school donors.	Unknown
Jan. 24, 2006	Univ. of WA Medical Center	Stolen laptops containing names, Social Security numbers, maiden names, birth dates, diagnoses and other personal data.	1,600
Jan. 25, 2006	Providence Home Services (OR)	Stolen backup tapes and disks containing Social Security numbers, clinical and demographic information. In a small number of cases, patient financial data was stolen.	365,000
Jan. 27, 2006	State of RI web site (www.RI.gov)	Hackers obtained credit card information in conjunction with names and addresses.	4,117

US2000 9491609.1

Jan. 31, 2006	Boston Globe and The Worcester Telegram & Gazette	Inadvertently exposed. Credit and debit card information along with routing information for personal checks printed on recycled paper used in wrapping newspaper bundles for distribution.	240,000 potentially exposed
Feb. 1, 2006	Blue Cross and Blue Shield of North Carolina	Inadvertently exposed. SSNs of members printed on the mailing labels of envelopes with information about a new insurance plan.	600
Feb. 4, 2006	FedEx	Inadvertently exposed. W-2 forms included other workers' tax information such as SSNs and salaries.	8,500
Feb. 9, 2006	Unknown retail merchants, apparently OfficeMax and perhaps others.	Hacking. Debit card accounts exposed involving bank and credit union accounts nationwide (including CitiBank, BofA, WaMu, Wells Fargo). [3/13/06 Crime ring arrested.]	200,000, although total number is unknown.
Feb. 9, 2006	Honeywell International	Exposed online. Personal information of current and former employees including Social Security numbers and bank account information posted on an Internet Web site.	19,000
Feb. 13, 2006	Ernst & Young (UK)	Laptop stolen from employee's car with customers' personal information including Social Security numbers.	38,000 BP employees in addition to Sun, Cisco and IBM employees.
Feb. 15, 2006	Dept. of Agriculture	Inadvertently exposed Social Security and tax identification numbers in FOIA request.	350,000
Feb. 15, 2006	Old Dominion Univ.	Exposed online. Instructor posted a class roster containing names and Social Security numbers to a web site.	601
Feb. 16, 2006	Blue Cross and Blue Shield of Florida	Contractor sent names and Social Security numbers of current and former employees, vendors and contractors to his home computer in violation of company policies.	27,000

Feb. 17, 2006	Calif. Dept. of Corrections, Pelican Bay (Sacramento, CA)	Inmates gained access to files containing employees' Social Security numbers, birth dates and pension account information stored in warehouse.	Unknown
Feb. 17, 2006	Mount St. Mary's Hospital (1 of 10 hospitals with patient info. stolen) (Lewiston, NY)	Two laptops containing date of birth, address and Social Security numbers of patients was stolen in an armed robbery in the New Jersey.	17,000
Feb. 18, 2006	Univ. of Northern Iowa	Hacking. Laptop computer holding W-2 forms of student employees and faculty was illegally accessed.	6,000
Feb. 23, 2006	Deloitte & Touche (McAfee employee information)	External auditor lost a CD with names, Social Security numbers and stock holdings in McAfee of current and former McAfee employees.	9,290
Mar. 1, 2006	Medco Health Solutions (Columbus, OH)	Stolen laptop containing Social Security numbers for State of Ohio employees and their dependents, as well as their birth dates and, in some cases, prescription drug histories.	4,600
Mar. 1, 2006	OH Secretary of State's Office	SSNs, dates of birth, and other personal data of citizens routinely posted on a State web site as part of standard business practice.	Unknown
Mar. 2, 2006	Olympic Funding (Chicago, IL)	3 hard drives containing clients names, Social Security numbers, addresses and phone numbers stolen during break in.	Unknown
Mar. 2, 2006	Los Angeles Cty. Dept. of Social Services (Los Angeles, CA)	File boxes containing names, dependents, Social Security numbers, telephone numbers, medical information, employer, W-2, and date of birth were left unattended and unshredded.	[Potentially 2,000,000, but number unknown] Not included in number below.
Mar. 2, 2006	Hamilton County Clerk of Courts (OH)	SSNs, other personal data of residents posted on county web site, were stolen and used to commit identity theft.	[1,300,000] Not included in number below.

US2000 9491609.1

Mar. 3, 2006	Metropolitan State College (Denver, CO)	Stolen laptop containing names and Social Security numbers of students who registered for Metropolitan State courses between the 1996 fall semester and the 2005 summer semester.	93,000
Mar. 5, 2006	Georgetown Univ. (Washington, D.C.)	Hacking. Personal information including names, birthdates and Social Security numbers of District seniors served by the Office on Aging.	41,000
Mar. 8, 2006	Verizon Communications (New York, NY)	2 stolen laptops containing employees' personal information including Social Security numbers.	"Significant number"
Mar. 8, 2006	iBill (Deerfield Beach, FL)	Dishonest insider or possibly malicious software linked to iBill used to post names, phone numbers, addresses, e-mail addresses, Internet IP addresses, logins and passwords, credit card types and purchase amount online. Credit card account numbers, expiration dates, security codes, and SSNs were NOT included, but in our opinion the affected individuals could be vulnerable to social engineering to obtain such information.	[17,781,462] Not included in total below.
Mar. 11, 2006	CA Dept. of Consumer Affairs (DCA) (Sacramento, CA)	Mail theft. Applications of DCA licensees or prospective licensees for CA state boards and commissions were stolen. The forms include full or partial Social Security numbers, driver's license numbers, and potentially payment checks.	"A small number"
Mar. 14, 2006	General Motors (Detroit, MI)	Dishonest insider keep Social Security numbers of co-workers to perpetrate identity theft.	100
Mar. 14 2006	Buffalo Bisons and Choice One Online (Buffalo, NY)	Hacker accessed sensitive financial information including credit card numbers names, passwords of customers who ordered items online.	Unknown
Mar. 15, 2006	Ernst & Young (UK)	Laptop lost containing the names, dates of birth, genders, family sizes, Social Security numbers and tax identifiers for current and previous IBM, Sun Microsystems, Cisco, Nokia and BP employees exposed.	Unknown
Mar. 16, 2006	Bananas.com (San Rafael, CA)	Hacker accessed names, addresses, phone numbers and credit card numbers of customers.	274
Mar. 23, 2006	Fidelity Investments (Boston, MA)	Stolen laptop containing names, addresses, birth dates, Social Security numbers and other information of 196,000 Hewlett Packard, Compaq and DEC retirement account customers was stolen.	196,000
Mar. 24, 2006	CA State Employment Development Division (Sacramento, CA)	Computer glitch sends state Employment Development Division 1099 tax forms containing Social Security numbers and income information to the wrong addresses, potentially exposing those taxpayers to identity theft.	64,000
Mar. 24, 2006	Vermont State Colleges (VT)	Laptop stolen containing Social Security numbers and payroll data of students, faculty and staff associated with the five-college system from as long ago as 2000.	14,000
Mar. 30, 2006	Marines (Monterey, CA)	Portable drive lost that contains personal information used for research on re-enlistment bonuses.	207,750
Mar. 30, 2006	Georgia Technology Authority (Atlanta, GA)	Hacker exploited security flaw to gain access to confidential information including Social Security numbers and bank-account details of state pensioners.	573,000
Mar. 30, 2006	Conn. Technical High School System (Middletown, CT)	Social Security numbers of students and faculty mistakenly distributed via email.	1,250
April 6, 2006	Progressive Casualty Insurance (Mayfield Village, OH)	Dishonest insider accessed confidential information, including names, Social Security numbers, birth dates and property addresses on foreclosure properties she was interested in buying.	13

US2000 9491609.1

April 7, 2006	DiscountDomain Registry.com (Brooklyn, NY)	Exposed online. Domain registrants' personal information including usernames, passwords and credit card numbers were accessible online.	"thousands of domain name registrations"
April 9, 2006	University of Medicine and Dentistry of New Jersey (Newark, NJ)	Hackers accessed Social Security numbers, loan information, and other confidential financial information of students and alumni.	1,850
April 12, 2006	Ross-Simons (Providence, RI)	Security breach exposed account and personal information of those who applied for its private label credit card. Information exposed includes private label credit card numbers and other personal information of applicants.	Unknown
April 14, 2006	Univ. of South Carolina (Columbia, SC)	Social Security numbers of students were mistakenly e-mailed to classmates.	1,400
April 21, 2006	University of Alaska, Fairbanks (Fairbanks, AK)	Hacker accessed names, Social Security numbers and partial e-mail addresses of current and former students, faculty and staff.	38,941
April 21, 2006	Ohio University Innovation Center (Athens, OH)	a server containing data including e-mails, patent and intellectual property files, and 35 Social Security numbers associated with parking passes was compromised.	Unknown
April 24, 2006	University of Texas' McCombs School of Business (Austin, TX)	Hackers accessed records containing names, biographical information and, in some cases, Social Security numbers and dates of birth of current and prospective students, alumni, faculty members, corporate recruiters and staff members.	197,000
April 24, 2006	Ohio University (Athens, OH)	Hackers accessed a computer system of the school's alumni relations department that included biographical information and 137,000 Social Security numbers of alum.	300,000
April 26, 2006	Purdue University (West Lafayette, IN)	Hacker accessed personal information including Social Security numbers of current and former graduate students, applicants to graduate school, and a small number of applicants for undergraduate scholarships.	1,351
April 26, 2006	Aetna -- health insurance records for employees of 2 members, including Omni Hotels and the Dept. of Defense NAF (Hartford, CT)	Laptop containing personal information including names, addresses and Social Security numbers of Dept. of Defense (35,253) and Omni Hotel employees (3,000) was stolen from an Aetna employee's car.	38,000
April 27, 2006	MasterCard (Potentially UK only)	Though MasterCard refused to say how the breach occurred, fraudsters stole the credit card details of holders in a major security breach.	[2,000] Not included in total below.
April 27, 2006	Long Island Rail Road (Jamaica, NY)	Data tapes containing personal information including names, addresses, Social Security numbers and salary figures of "virtually everyone" who worked for the agency was lost by delivery contractor Iron Mountain while enroute. Data tapes belonging to the U.S. Department of Veterans Affairs may also have been affected.	17,000
April 28, 2006	Ohio's Secretary of State (Cleveland, OH)	The names, addresses, and Social Security numbers of potentially millions of registered voters in Ohio were included on CD-ROMs distributed to 20 political campaign operations for spring primary election races. The records of about 7.7 million registered voters are listed on the CDs, but it's unknown how many records contained SSNs, which were not supposed to have been included on the CDs.	"Potentially millions of registered voters"
April 28, 2006	Dept. of Defense (Washington, DC)	Hacker accessed a Tricare Management Activity (TMA) public server containing personal information about military employees.	Unknown
May 2,	Georgia State Government	Government surplus computers	Unknown

US2000 9491609.1

2006	(Atlanta, GA)	that sold before their hard drives were erased contained credit card numbers, birth dates, and Social Security numbers of Georgia citizens.	
May 4, 2006	Idaho Power Co. (Boise, ID)	Four company hard drives were sold on eBay containing hundreds of thousands of confidential company documents, employee names and Social Security numbers, and confidential memos to the company's CEO.	Unknown
May 4, 2006	Ohio University Hudson Health Center (Athens, OH)	Names, birth dates, Social Security numbers and medical information were accessed in records of students dating back to 2001, plus faculty, workers and regional campus students.	60,000
May 2006	Ohio University (Athens, OH)	A breach was discovered on a computer that housed IRS 1099 forms for vendors and independent contractors for calendar years 2004 and 2005.	2,480
May 2006	Ohio University (Athens, OH)	A breach of a computer that hosted a variety of Web-based forms, including some that processed on-line business transactions. Although this computer was not set up to store personal information, investigators did discover files that contained fragments of personal information, including Social Security numbers. The data is fragmentary and it is not certain if the compromised information can be traced to individuals. Also found on the computer were 12 credit card numbers that were used for event registration.	Unknown
May 5, 2006	Dept. of Veteran Affairs (Washington, D.C.)	A data tape disappeared from a VA facility in Indianapolis, IN that contained information on legal cases involving U.S. veterans and included veterans' Social Security numbers, dates of birth and legal documents.	16,500
May 5, 2006	Wells Fargo (San Francisco, CA)	Computer containing names, addresses, Social Security numbers and mortgage loan deposit numbers of existing and prospective customers may have been stolen while being delivered from one bank facility to another.	Unknown
May 12, 2006	Mercantile Potomac Bank (Gaithersburg, MD)	Laptop containing confidential information about customers, including Social Security numbers and account numbers was stolen when a bank employee removed it from the premises, in violation of the bank's policies. The computer did not contain customer passwords, personal identification numbers (PIN numbers) or account expiration dates.	48,000
May 19, 2006	American Institute of Certified Public Accountants (AICPA) (New York, NY)	An unencrypted hard drive containing names, addresses and Social Security numbers of AICPA members was lost when it was shipped back to the organization by a computer repair company.	330,000 [Updated 6/16/06]
May 19, 2006	Unknown retail merchant	Visa, MasterCard, and other debit and credit card numbers from banks across the country were stolen when a national retailer's database was breached. No names, Social Security numbers or other personal identification were taken.	Unknown
May 22, 2006	Dept. of Veterans Affairs (Washington, DC)	On May 3, data of all American veterans who were discharged since 1975 including names, Social Security numbers, dates of birth and in many cases phone numbers and addresses, were stolen from a VA employee's home. Theft of the laptop and computer storage device included data of 26.5 milliion veterans. The data did not contain medical or financial information, but may have disability numerical rankings. **UPDATE:** An additional 2.1 million active and reserve service members were added to the total number of affected individuals June 1st. **UPDATE** (6/29/06): The stolen	28,600,000

US2000 9491609.1

		laptop computer and the external hard drive were recovered. **UPDATE** (7/14/06): FBI claims no data had been taken from stolen computer.	
May 23, 2006	Univ. of Delaware (Newark, DE)	Security breach of a Department of Public Safety computer server potentialy exposes names, Social Security numbers and driver's license numbers.	1,076
May 23, 2006	M&T Bank (Buffalo, NY)	Laptop computer, owned by PFPC, a third party company that provides record keeping services for M & T's Portfolio Architect accounts was stolen from a vehicle. The laptop contained clients' account numbers, Social Security numbers, last name and the first two letters of their first name.	Unknown
May 24, 2006	Sacred Heart Univ. (Fairfield, CT)	It was discovered on May 8th that a computer containing personal information including names, addresses and Social Security numbers was breached.	Unknown
May 24, 2006	American Red Cross, St. Louis Chapter (St. Louis)	Dishonest employee had access to Social Security numbers of donors to call urging them to give blood again. The employee misused the persoal information of at least 3 people to perpetrate identity theft and had access to the personal information of 1 million donors.	1,000,000
May 25, 2006	Vystar Credit Union (Jacksonville, FL)	Hacker gained access to member accounts "a few weeks ago" and stole personal information including names, addresses, birth dates, mother's maiden names, SSNs and/or email addresses.	Approx. 34,400 ("less than 10% of its 344,000 members")
May 30, 2006	Texas Guaranteed Student Loan Corp. (Round Rock, TX) via subcontractor, Hummingbird (Toronto, Canada)	Texas Guaranteed (TG) was notified by subcontractor Hummingbird that an employee had lost a piece of equipment containing names and Social Security numbers of TG borrowers.	1,300,000
May 30, 2006	Florida Int'l Univ. (Miami, FL)	Hacker accessed a database that contained personal information, such as student and applicant names and Social Security numbers.	"thousands"
June 1, 2006	Miami University (Oxford, OH)	An employee lost a hand-held personal computer containing personal information of students who were enrolled between July 2001 and May 2006.	851
June 1, 2006	Ernst & Young (UK)	A laptop containing names, addresses and credit or debit card information of Hotels.com customers was stolen from an employee's car in Texas.	243,000
June 1, 2006	Univ. of Kentucky (Lexington, KY)	Personal information of current and former University of Kentucky employees including Social Security numbers was inadvertently accessible online for 19 days last month.	1,300
June 2, 2006	Buckeye Community Health Plan (Columbus, OH)	Four laptop computers containing customer names, Social Security numbers, and addresses were stolen from the Medicaid insurance provider.	72,000
June 2, 2006	Ahold USA (Landover, MD) Parent company of Stop & Shop, Giant stores and Tops stores via subcontractor Electronic Data Systems (Plano, TX)	An EDS employee lost a laptop computer during a commercial flight that contained pension data of former employees of Ahold's supermarket chains including Social Security numbers, birth dates and benefit amounts.	Unknown
June 2, 2006	YMCA (Providence, RI)	Laptop computer containing personal information of members was stolen. The information included credit card and debit card numbers, checking account information, Social Security numbers, the names and addresses of children in daycare programs and medical information about the children, such as allergies and the medicine they take, though the type of stolen information about each person varies.	65,000
June 2,	Humana	Personal information of Humana	17,000

2006	(Louisville, KY)	customers enrolled in the company's Medicare prescription drug plans could have been compromised when an insurance company employee called up the data through a hotel computer and then failed to delete the file.	
June 5, 2006	Internal Revenue Service (Washington, DC)	A laptop computer containing personal information of employees and job applicants, including fingerprints, names, Social Security numbers, and dates of birth, was lost during transit on an airline flight	291
June 6, 2006	Univ. of Texas (El Paso, TX)	Students demonstrated that student body and faculty elections could be rigged by hacking into student information including Social Security numbers.	4,719
June 8, 2006	Univ. of Michigan Credit Union (Ann Arbor, MI)	Paper documents containing personal information of credit union members were stolen from a storage rooms. The documents were supposed to have been digitally imaged and then shredded. Instead, they were stolen and used to perpetrate identity theft.	5,000
June 11, 2006	Denver Election Commission (Denver, CO)	Records containing personal information on more than 150,000 voters are missing at city election offices. The microfilmed voter registration files from 1989 to 1998 were in a 500-pound cabinet that disappeared when the commission moved to new offices in February. The files contain voters' Social Security numbers, addresses and other personal information.	150,000
June 12, 2006	U.S. Dept. of Energy (Washington, D.C.)	Names, Social Security numbers, security clearance levels and place of employment for mostly contract employees who worked for National Nuclear Security Administration may have been compromised when a hacker gained entry to a computer system at a service center in Albuquerque, N.M. eight months ago.	1,502
June 13,	Minn. State Auditor	Three laptops possibly containing	493
2006	(St. Paul, MN)	Social Security numbers of employees and recipients of housing and welfare benefits along with other personal information of local governments the auditor oversees have gone missing.	
June 13, 2006	Oregon Dept. of Revenue (Salem, OR)	Electronic files containing personal data of Oregon taxpayers may have been compromised by an ex-employee's downloaded a contaminated file from a porn site. The "trojan" attached to the file may have sent taxpayer information back to the source when the computer was turned on.	2,200
June 13, 2006	U.S. Dept of Energy, Hanford Nucear Reservation (Richland, WA)	Current and former workers at the Hanford Nuclear Reservation that their personal information may have been compromised, after police found a 1996 list with workers' names and other information in a home during an unrelated investigation.	4,000
June 14, 2006	American Insurance Group (AIG), Midwest Office (New York, NY)	The computer server was stolen on March 31 containing personal information including names, Social Security numbers and tens of thousands of medical records.	930,000
June 14, 2006	Western Illinios Univ. (Macomb, IL)	On June 5th, a hacker compromised a University server that contained names, addresses, credit card numbers and Social Security numbers of people connected to the University. [**UPDATE 7/5/06**. Number affected reduced from 240,000.]	180,000
June 16, 2006	Union Pacific (Omaha, NE)	On April 29th, an employee's laptop was stolen that contained data for current and former Union Pacific employees, including names, birth dates and Social Security numbers.	30,000
June 16, 2006	NY State Controller's Office (Albany, NY)	State controller data cartridge containing payroll data of employees who work for a variety of state agencies was lost during shipment. The data contained names, salaries, Social Security numbers and home addresses.	1,300

June 16, 2006	ING (Miami, FL)	Two ING laptops that carried sensitive data affecting of Jackson Health System hospital workers were stolen in December 2005. The computers, belonging to financial services provider ING, contained information gathered during a voluntary life insurance enrollment drive in December and included names, birth dates and Social Security numbers.	8,500
June 16, 2006	Univ. of Kentucky (Lexington, KY)	The personal data of current and former students including classroom rosters names, grades and Social Security numbers was reported stolen on May 26 following the theft of a professor's flash drive..	6,500
June 17, 2006	ING (Washington, D.C.)	Laptop stolen from employee's home containing retirement plan information including Social Security numbers of D.C. city employees.	13,000
June 17, 2006	Automatic Data Processing (ADP) (Roseland, NJ)	Personal and payroll information of workers were intended to be faxed between ADP offices and were mistakenly sent to a third party.	80
June 17, 2006	CA Dept. of Health Services (CDHS) (Sacramento, CA)	CDHS documents were inappropriately emptied from an employee's cubicle on June 5 and 9 rather than shredded. The documents contained state employees and other individuals applying for employment with the state including names, addresses, Social Security numbers and home and work telephone numbers. They were mostly expired state employment certification lists, but also included requests for personnel action, copies of e-mail messages and handwritten notes.	1,550
June 20, 2006	Equifax (Atlanta, GA)	On May 29, a company laptop containing employee names and partial and full Social Security numbers was stolen from an employee.	2,500
June 20, 2006	Univ. of Alabama (Birmingham, AL)	In February a computer was stolen from a locked office of the kidney transplant program at the University of Alabama at Birmingham that contained confidential information of donors, organ recipients and potential recipients including names, Social Security numbers and medical information.	9,800
June 21, 2006	U.S. Dept. of Agriculture (USDA) (Washington, D.C.)	During the first week in June, a hacker broke into the Department's computer system and may have obtained names, Social Security numbers and photos of current and former employees and contractors.	26,000
June 21, 2006	Cape Fear Valley Health System (Fayetteville, NC)	Portable computer containing personal information of more than 24,000 people was stolen from ambulance of Cumberland Co. Emergency Medical Services on June 8th. It contained information on people treated by the EMS, including names, addresses, and birthdates, plus SSNs of 84% of those listed.	24,350
June 22, 2006	Fed. Trade Comm. (FTC) (Washington, D.C.)	Two laptop computers containing personal and financial data were stolen from an employee's vehicle. The data included names, addresses, Social Security numbers, dates of birth, and in some instances, financial account numbers gathered in law enforcement investigations.	110
June 23, 2006	San Francisco State Univ. (San Francisco, CA)	a faculty member's laptop was stolen from a car on June 1 that contained personal information of former and current students including Social Security numbers, and names and ins some instance, phone numbers and grade point averages.	3,000
June 23, 2006	U.S. Navy (Washington, D.C.)	Navy personnel were notified on June 22 that a civilian web site contained files with personal information of Navy members and dependents including names, birth dates and Social Security numbers.	30,000

US2000 9491609.1

June 23, 2006	CA Dept. of Health Services (CDHS) (Sacramento, CA)	On June 12, a box of Medi-Cal forms from December 2005 were found in the cubicle of a CDHS employee. The claim forms contained the names, addresses, Social Security numbers and prescriptions for beneficiaries or their family members.	323
June 23, 2006	Catawba County Schools (Newton, NC)	On June 22, it was discovered that a web site posted names, Social Security numbers, and test scores of students who had taken a keyboarding and computer applications placement test during the 2001-02 school year. **UPDATE:** The web site containing the data has been removed.	619
June 23, 2006	King County Records, Elections, and Licensing Services Division (Seattle, WA)	Social Security numbers for potentially thousands of current and former county residents may be exposed on the agency's web site. Residents can request that the image of any document that contains a Social Security number, Mother's Maiden Name or Drivers License be removed. Officials state that they are unable to alter original public documents and cannot choose to not record documents presented for recording.	Unknown
June 27, 2006	Gov't Accountability Office (GAO) (Washington, D.C.)	Data from audit reports on Defense Department travel vouchers from the 1970s were inadvertently posted online and included some service members' names, Social Security numbers and addresses. The agency has subsequently removed the information.	"Fewer than 1,000" [1,000 used in total]
June 28, 2006	AAAAA Rent-A-Space (Colma, CA)	Customer's account information including name, address, credit card, and Social Security number was easily accessible due to a security gap in its online payment system.	13,000
June 29, 2006	AllState Insurance Huntsville branch (Huntsville, AL)	Over Memorial Day weekend, a computer containing personal data including images of insurance policies, correspondence and Social Security numbers was stolen.	2,700
June 29, 2006	Nebraska Treasurer's Office (Lincoln, NE)	A hacker broke into a child-support computer system and may have obtained names, Social Security numbers and other information such as tax identification numbers for 9,000 businesses.	309,000
June 29, 2006	Minnesota Dept. of Revenue (St. Paul, MN)	On May 16, a package containing a data tape used to back up the regional office's computers went missing during delivery. The tape contained personal information including individuals' names, addresses, and Social Security numbers. **UPDATE 7-20-06**: The package was reported delivered 2 months later, but apparently had been temporarily lost by the U.S. Postal Service.	50,400
June 30, 2006	Nat'l Institutes of Health Federal Credit Union (Rockville, MD)	NIHFCU is investigating with law enforcement the identity theft of some of its 41,000 members. No details given on type of information stolen, or how it was stolen.	"Very few" of 41,000 members affected [not included in total]
July 1, 2006	American Red Cross, Farmers Branch (Dallas, TX)	Sometime in May, 3 laptops were stolen, one of them containing encrypted personal information including names, SSNs, dates of birth, and medical information of all regional donors. They also report losing a laptop with encrypted donor information in June 2005.	Unknown
July 5, 2006	Bisys Group Inc. (Roseland, NJ)	Personal details about 61,000 hedge fund investors were lost when an employee's truck carrying backup tapes was stolen. The data included SSNs of 35,000 individuals. The tapes were being moved from one Bisys facility to another on June 8 when the theft occurred.	61,000
July 6, 2006	Automated Data Processing (ADP) (Roseland, NJ)	Payroll service company ADP gave scam-artist names, addresses, and	"Hundreds of thousands" [not

		number of shares held of investors, although apparently not SSNs or account numbers. The leak occurred from Nov. '05 to Feb. '06 and involved individual investors with 60 companies including Fidelity, UBS, Morgan Stanley , Bear Stearns, Citigroup, Merrill Lynch.	included in total]
July 7, 2006	University of Tennessee (866) 748-1680	Hacker broke into UT computer containing names, addresses and SSNs of about 36,000 past and current employees. Intruder apparently used computer from Aug. '05 to May '06 to store and transmit movies.	36,000
July 7, 2006	Nat'l Association of Securities Dealers (NASD) (Boca Raton, FL)	Ten laptops were stolen on Feb. 25 '06 from NASD investigators. They included SSNs of securities dealers who were the subject of investigations involving possible misconduct. Inactive account numbers of about 1,000 consumers were also contained on laptops.	73
July 7, 2006	Naval Safety Center	SSNs and other personal information of naval and Marine Corps aviators and air crew, both active and reserve, were exposed on Center web site and on 1,100 computer discs mailed to naval commands.	"more than 100,000"
July 7, 2006	Montana Public Health and Human Services Dept. (Helena, MT)	A state government computer was stolen from the office of a drug dependency program. during a 4th of July break-in. It was not known if sensitive information such as SSNs was compromised.	Unknown
July 13, 2006	Moraine Park Technical College (Beaver Dam, Fond du Lac, & West Bend, WI)	Computer disk (CD) with personal information of 1,500 students was reported missing. Information includes names, addresses, phone numbers & SSNs of apprenticeship students back to 1993.	1,500
July 14, 2006	Northwestern Univ. (Evanston, IL) (888-209-0097)	Files containing names and some personal information including SSNs were on 9 desktop computers that had been accessed by unauthorized persons outside the University. The computers were	"As many as 17,000 individuals' records" exposed

		in the Office of Admissions and Financial Aid Office.	
July 14, 2006	University of Iowa (Davenport, IA)	Laptop computer containing personal information of current and former MBA students was stolen. Data files included SSNs and some contact info.	280
July 14, 2006	Treasurer's computer in Circuit Court Clerk's office (Hampton, VA)	Public computer in city government building containing taxpayer information was found to display SSNs of many residents -- those who paid personal property and real estate taxes. It was shut down and confiscated by the police on July 12th.	"Over 100,000 records" (The number containing SSNs is not known yet and not included in total below.)
July 18, 2006	Nelnet Inc. (Lincoln, NE) (800) 552-7925	Computer tape containing personal information of student loan customers was lost when shipped via UPS. The loans were previously serviced by College Access Network	188,000
July 18, 2006	CS Stars, subsidiary of insurance company Marsh Inc. (Chicago, IL)	On May 9, CS Stars lost track of a personal computer containing records of more than a half million New Yorkers who made claims to a special workers' comp fund. The lost data includes SSNs and date of birth but apparently no medical information.	540,000
July 18, 2006	U.S. Dept. of Agriculture (Wellington, KS)	Laptop computer and printout containing names, addresses and SSNs of 350 employees was stolen from an emplolyee's car and later recovered.	350
July 24, 2006	New York City Dept. of Homeless Services	The personal information of 8,400 homeless persons, including SSNs, was leaked in an e-mail attachment July 21, when accidentally sent to homeless advocates and city officials.	8,400
July 25, 2006	Armstrong World Industries (Lancaster Co., PA)	A laptop containing personal information of current and former employers was stolen. The computer was in the possession of the company's auditor, Deloitte & Touche. Data included names, home addresses, phone numbers, SSNs, employee ID numbers,	12,000

US2000 9491609.1

		salary data, and bank account numbers of employees who have their checks directly deposited.	
July 25, 2006	Georgetown University Hospital(Washington, DC)	Patient data was exposed online via the computers of an e-prescription provider, InstantDx. Data included names, addresses, SSNs, and dates of birth, but not medical or prescription data. GUH suspended the trial program with InstantDX.	"between 5,600 and 23,000 patients were affected" (23,000 added to total below)
July 25, 2006	Old Mutual Capital Inc., subsidiary of United Kingdom-based financial services firm Old Mutual PLC	Laptop was stolen sometime in May containing personal information of clients, including names, addresses, account numbers and some SSNs.	6,500 fund shareholders
TOTAL number of records containing sensitive personal information involved in security breaches			**89,928,162**

The above table used with permission of the Privacy Rights Clearinghouse, www.privacyrights.org.

Privacy, Spam & Spyware 2006

Section 311 – ACC Annual Meeting

October 23, 2006

Examples of Definitions of Personal Information

Business Example:

"Personally Identifiable Information" shall include data or information in any form that can, by itself or in combination with other available data or information, identify an individual.

Nevada Revised Statute 205.4617:

1. Except as otherwise provided in subsection 2, "personal identifying information" means any information designed, commonly used or capable of being used, alone or in conjunction with any other information, to identify a living or deceased person, including, without limitation:

(a) The current or former name, driver's license number, identification card number, social security number, checking account number, savings account number, credit card number, debit card number, financial services account number, date of birth, place of employment and maiden name of the mother of a person.

(b) The unique biometric data of a person, including, without limitation, the fingerprints, facial scan identifiers, voiceprint, retina image and iris image of a person.

(c) The electronic signature, unique electronic identification number, address or routing code, telecommunication identifying information or access device of a person.

(d) The personal identification number or password of a person.

(e) The alien registration number, government passport number, **employer identification number**, taxpayer identification number, Medicaid account number, food stamp account number, medical identification number or health insurance identification number of a person.

(f) The number of any professional, occupational, recreational or governmental license, certificate, permit or membership of a person.

(g) The number, code or other identifying information of a person who receives medical treatment as part of a confidential clinical trial or study, who

participates in a confidential clinical trial or study involving the use of prescription drugs or who participates in any other confidential medical, psychological or behavioral experiment, study or trial.

(h) The utility account number of a person.

2. To the extent that any information listed in subsection 1 is designed, commonly used or capable of being used, alone or in conjunction with any other information, to identify an artificial person, "personal identifying information" includes information pertaining to an artificial person.

Illinois Bill Public Act 094-0036.

"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 or redacted:

(1) Social Security number.

(2) Driver's license number or State identification card number

(3) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, 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.

Limited Use of Social Security Number

As a side note, as evidence of the emerging trend towards increased protection of Social Security Numbers through the implementation of restrictions on use as a general identifier, **California Labor Code Section 226** reads in part:

Every employer shall, semimonthly or at the time of each payment of wages, furnish each of his or her employees, either as a detachable part of the check, draft, or voucher paying the employee's wages, or separately when wages are paid by personal check or cash, an accurate itemized statement in writing showing: ….

(7) the name of the employee and his or her social security number, except that by January 1, 2008, only the last four digits of his or her social security number or an employee identification number other than a social security number may be shown on the itemized statement …

Privacy, Spam & Spyware 2006

Section 311 – ACC Annual Meeting

October 23, 2006

Examples of FTC Actions

FTC Announces First Case Highlighting Application of Do Not Call Provisions to Affiliates

Discount Health Card Seller and Its Telemarketer to Pay Combined $350,000 Penalty for Do Not Call Violations

A seller of discount health and prescription drug cards and its telemarketer will pay civil penalties of $300,000 and $50,000, respectively, to settle Federal Trade Commission charges that they have been violating the Do Not Call (DNC) provisions of the Commission's Telemarketing Sales Rule (TSR), and will be prohibited from similar conduct in the future, the agency announced today. At the Commission's request, the U.S. Department of Justice (DOJ) filed the complaint and proposed stipulated consent orders in Federal District Court in New York City. This is the Commission's first case to highlight the application of DNC provisions to corporate affiliates

(http://www.ftc.gov/opa/2006/06/phaseone.htm)

Internet Marketers Settle FTC Charges

Spam Failed to Give Consumers the Ability to Opt Out of Future Messages

The Federal Trade Commission has charged two Internet marketers with violating the CAN-SPAM Act by failing to offer an opt-out method or honor consumers' right to opt out of receiving future marketing mailings within 10 days of making the request. One marketer also failed to include a valid physical postal address, which also is required by the CAN-SPAM Act. Settlements with the marketers prohibit future violations of the Act and provide for civil penalties totaling more than $32,000. (This is the IKodak/Ofoto action)

The FTC charged that Kodak Imaging Network, formerly Ofoto, Inc., sent a commercial e-mail message to more than two million recipients that failed to contain an opt-out mechanism, failed to disclose in the e-mail message that consumers have the right to opt-out of receiving further mailings, and failed to include a valid physical postal address, as required by law.

(http://www.ftc.gov/opa/2006/05/ofotokodak.htm)

Court Halts Spyware Operations

One Operator to Pay More Than $4 Million; Another Ordered to Stop Collecting

Consumers Personal Information

An operation that deceptively downloaded spyware onto unsuspecting consumers' computers, changing their settings and hijacking their search engines, has been halted by a federal court at the request of the Federal Trade Commission. The judge has ordered the operators to give up to more than $4 million in ill-gotten gains. The court also ordered a halt to another spyware operator's stealthy downloads and barred the collection of consumers' personal information, pending trial.

(http://www.ftc.gov/opa/2006/05/seismic.htm)

FTC Slams Spammer in Pocketbook

"FreeFlixTix" Scheme Threatened Reliability of E-mail

An Internet marketer will pay a $900,000 civil penalty for violating the CAN-SPAM Act, the largest penalty yet for illegal spam, according to the Federal Trade Commission. The company also is permanently prohibited from its unlawful practices, according to a consent decree signed by the company.

According to the FTC, since July 2002, San Francisco-based Jumpstart Technologies LLC, has operated as an Internet marketer, providing direct marketing opportunities for its advertising partners and collecting marketing information to sell to third parties. The FTC's complaint alleges that in its FreeFlixTix promotion, Jumpstart violated the law by disguising its commercial e-mails as personal messages, and by misleading consumers as to the terms and conditions of the promotion.

According to the complaint, Jumpstart violated provisions of the CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) Act by sending commercial e-mails with false or misleading subject and "from" lines, sending e-mails more than 10 business days after receiving an opt-out request from consumers, not clearly identifying messages as advertising or solicitations, and not clearly informing recipients that they could opt out of receiving more e-mails. Its unfair or deceptive marketing also violated the FTC Act.

(http://www.ftc.gov/opa/2006/03/freeflixtix.htm)

Book Club Direct Marketer to Pay $680,000 for Do Not Call Violations

Book-of-the-Month Club Partnership Called Over 100,000 Consumers on DNC Registry; Continued Calling Customers Who Specifically Asked Not to be Called

In the most recent case brought against a company for failing to stop calling consumers who asked to be put on the company's own do not call list, the Federal Trade Commission today announced that book club direct marketer Bookspan will pay a $680,000 civil penalty to settle the Commission's charges. The Commission also alleged that Bookspan called more than 100,000 consumers on the National Do Not Call (DNC) Registry. The complaint and proposed order were filed in court today by the U.S. Department of Justice on the Commission's behalf. The FTC alleged that

Bookspan, a partnership of Book of the Month Club Holdings, LLC and Doubleday Direct, Inc., called tens of thousands of consumers who previously asked to be put on its own ("entity-specific") do not call list, and also unlawfully called consumers on the DNC Registry. The court order settling the case bars the company from violating the FTC Act and Telemarketing Sales Rule (TSR) in the future. The DNC Rule is part of the Commission's TSR provisions.

(http://www.ftc.gov/opa/2006/02/bookspan.htm)

CardSystems Solutions Settles FTC Charges

Tens of Millions of Consumer Credit and Debit Card Numbers Compromised

In the largest known compromise of financial data to date, CardSystems Solutions, Inc. and its successor, Solidus Networks, Inc., doing business as Pay By Touch Solutions, have agreed to settle Federal Trade Commission charges that CardSystems' failure to take appropriate security measures to protect the sensitive information of tens of millions of consumers was an unfair practice that violated federal law. According to the FTC, the security breach resulted in millions of dollars in fraudulent purchases. The settlement will require CardSystems and Pay By Touch to implement a comprehensive information security program and obtain audits by an independent third-party security professional every other year for 20 years.

(http://www.ftc.gov/opa/2006/02/cardsystems_r.htm)

Privacy, Spam & Spyware 2006

Section 311 – ACC Annual Meeting

October 23, 2006

Online Privacy Resources

1. National Conference of State Legislatures
   http://www.ncsl.org/programs
   Offers a variety of services to help lawmakers tailor policies to work for states and constituents; provides summary of certain state laws, including privacy law.

2. Federal Trade Commission
   http://www.consumer.gov/idtheft/
   The FTC identity theft Web page looks at how identity thieves work, provides government reports and Congressional testimony, law enforcement updates and links to other identity theft sites. The page also provides statistics compiled by the agency.

3. American Bankers Association Education Foundation
   http://www.aba.com/Consumer+Connection/CNC_contips_idtheft.htm
   The American Bankers Association Education Foundation's Consumer Connection provides resources about banking and personal finance.

4. Credit Union National Association
   http://www.cuna.org/initiatives/idtheft.html
   CUNA (Credit Union National Association), based in Washington, D.C., and Madison, Wisconsin, is a national trade association serving America's credit unions and provides resources to combat identity theft.

5. Identity Theft Resource Center
   http://www.idtheftcenter.org/index.shtml
   A non-profit organization that provides consumer and victim support.

6. National Consumers League
   http://www.nclnet.org
   The nation's oldest consumer organization, the National Consumers League identifies and protects economic and social interests of consumers. NCL provides governments, businesses and organizations a consumer perspective on identity theft and many other issues.

7. Privacy Rights Clearinghouse
   http://www.privacyrights.org/identity.htm
   The clearinghouse Web page provides a list of resources for more information about identity theft and lists of publications to assist victims of identity theft.

8. Bank of America Privacy Pages
   http://www.bankofamerica.com/privacy/

9. U.S. Department of Justice
   http://usdoj.gov/criminal/fraud/idtheft.html
   This DOJ Web page provides questions and answers to the most common identity theft queries. There are strategies to avoid becoming a victim of identity theft and strategies for dealing with identity theft after it occurs.

10. U.S. Social Security Administration
    http://www.ssa.gov/pubs/idtheft.htm
    The Social Security Administration gives identity theft hotline numbers; information on reclaiming identity; Social Security card replacement; correcting records and, in certain circumstances, getting a new Social Security number.

11. http://www.consumer.gov/idtheft/
    The US federal government consumer information gateway.

US2000 9485972.1

Privacy, Spam & Spyware 2006

Session 311 – ACC Annual Meeting

Donna K. Lewis

Kilpatrick Stockton LLP

October 23, 2006

A. Introduction

As both businesses and consumers increase their reliance on technology, the concepts of privacy and security are beginning to merge. Privacy laws generally recognize an individual's right to privacy in those areas where the individual has a reasonable expectation of and interest in privacy and operate to effectively restrict or prohibit activities that would compromise that interest. As will be discussed in greater detail below, privacy laws have evolved historically as a means to protect individuals from the potential harm associated with the misuse of private information. In the same way that technology has enabled both consumers and businesses to build efficiencies and take advantage of new products and services, it has also enabled the creation of huge repositories of stored data and new windows into historically private and perhaps anonymous transactions. While this electronic data may be considered "private" to the individual, it is increasingly being recognized as extremely valuable to the underlying business in its electronic form and as part of a much larger collection of data. Among other things, vast amounts of electronic personal data can be aggregated and analyzed to reveal trends in consumer behavior, develop targeted marketing messages, launch new products and services, and connect with customers in a more personalized way. Accordingly, as business changes with technology innovation and proliferation, there are new economic reasons to collect data and obtain broad usage rights from customers and simultaneously protect that data from unauthorized access or use by third parties. Consumer trust is critical to the ability to obtain broad usage rights and the implementation of appropriate information security measures is critical to the protection of private information. As a result, it is not surprising that the dominant trends in new and proposed privacy legislation are to grant consumers greater rights of control over the use of their personal data in the marketplace and to encourage those who collect data to implement procedures designed to secure the data and minimize the risk of unauthorized access to and use of such data.

B. Overview of Common Law Privacy Tort

As a basic principle of law, the right to privacy includes four separate components: (i) the right to prevent intrusion upon personal solitude; (ii) the right to prevent publications that place one in a false light and would be offensive to a reasonable person; (iii) the right to prevent public disclosure of embarrassing private facts; and (iv) the right to prevent unauthorized commercial exploitation of a name or likeness (i.e., the right of publicity). The first three rights generally involve a right to be left alone, whereas the fourth right, the right of publicity, centers on the commercial nature of one's name and likeness and establishes a right to control the commercial use of the same, a right typically afforded to one whose name or image has some commercial value. The "false light" tort is generally characterized by a concern for accuracy under common law and in many privacy statutes, while the right to be left alone is characterized as a concern that even truthful disclosure of private facts about an

individual is inappropriate. The focus of this latter concern generally balances the right of the individual against the perceived right of society to have access to that information. Finally, the "embarrassing facts" privacy tort involves a finding of the disclosure of embarrassing facts that are offensive in nature coupled with the lack of a legitimate public interest in the disclosure of such facts.

In addition to the line of cases providing protection against harmful disclosure of personal information, courts have historically provided protection from government invasions of citizen privacy, an effort that is rooted in the Fourth Amendment. Over time, this protection has expanded beyond the Fourth Amendment search and seizure protection to recognize a more general right against government-compelled disclosures of personal matters, which has been followed by various statutory provisions limiting the power of the government to compel disclosure of personal information and applying restrictions on use of that information once disclosed. These protections are largely responsive to the reality that the government is in a unique position to force disclosure of personal information without any concern for marketplace or consumer repercussions.

Finally, although there is no right to privacy set forth in the Constitution, the Court held in a series of cases that the Constitution protected a "zone of privacy" designed to safeguard privacy in connection with making certain kinds of important decisions. In Whalen v. Roe, [1] the Court indicated that the constitutionally protected "zone of privacy" also extends to an individual's interest in avoiding disclosure of personal matters, arguably defining a constitutionally based right of information privacy. While the Court has not developed this right of information privacy, this right has been recognized by a majority of circuit courts.

[1] 433 U.S. 425 (1977).

C. Overview of Existing Federal Laws

Over time, federal laws have been developed to address the collection and use of personal information by the private sector to provide protection in fairly narrow areas. Current privacy laws can be grouped into several areas, namely data breach/notification, health information privacy, identity theft, online privacy and unsolicited commercial communication. The growth of federal privacy statutory protection correlates with the proliferation of technology, starting with the rise of the computer and its impact on data collection, use and storage, and continuing with technology's impact on communications and business processes. Additionally, privacy protection can be found in certain industry-specific laws, such as the Cable Communication Policy Act of 1984,[2] which protects the privacy of cable records and requires notification about collection practices and limitations on disclosure. The fact that privacy laws are dispersed throughout various laws makes compliance particularly challenging. Additionally, as certain industries converge, it is unclear how historically separate industry–specific regulations, such as telecom and cable, will be reconciled to the extent that they are inconsistent. While any such inconsistencies will certainly present compliance issues, perhaps more importantly, they will present business challenges. As a result of the historically limited scope of privacy laws targeted to the private sector, many companies may have concluded that the privacy laws are not applicable to them and, therefore, there is no need to allocate any resources towards a

[2] 42 U.S.C. § 551.

privacy compliance program. As will be discussed over the course of this paper, there are, in fact, legitimate legal and business reasons to rethink such a position and give serious consideration to developing a data governance and security policy and a compliance and enforcement program.

One of the earliest laws designed to address data collection and use issues by the private sector was the Fair Credit Reporting Act[3] ("**FCRA**"). This law was designed to promote accuracy, fairness, and privacy of information in the files maintained by consumer reporting agencies or credit bureaus. By definition, this law applies to those entities in the business of gathering and selling information about consumers to creditors, employers, landlords and other businesses. As such, the law focuses on establishing procedures designed to correct inaccuracies and protect consumers from harmful uses of that data. The Gramm-Leach-Bliley Act of 1999[4] ("**GLB**") allows traditional financial institutions and other entities significantly engaged in financial activities with different branches or affiliates engaging in different services to share the "nonpublic personal information" data collected by a branch across other branches. While customers must be notified of the internal sharing practice, they cannot object to the internal sharing of the data. Customers, may, however, opt-out of any sharing of their data with third party companies. Whether an opt-in approach would be more protective of consumers rights and, therefore, preferable, is still a matter of some debate as such an approach may reduce the amount of data collected and available.

[3] 15 U.S.C. § 1681 (1970).
[4] 15 U.S.C. §§ 6801-6809 (1999).

The Health Insurance Portability and Accountability Act of 1996[5] ("**HIPAA**") was passed to simultaneously encourage and enable cost savings by health care companies associated with the creation and use of electronic health information records and provide for the security and confidentiality of patient information. HIPAA applies to health plans, health care clearing houses and health care providers who conduct certain financial and administrative transactions electronically. Given that HIPAA's protections are limited to medical records held by certain defined types of medical groups, HIPAA does not, therefore, protect all databases containing health information. As a result of the fact that HIPAA applies only to certain types of record holders, HIPAA does not provide full and complete protection of all medical information.

Although specific to online privacy, the Children's Online Privacy Protection Act[6] ("**COPPA**") was adopted in recognition of the specific privacy issues associated with children in an online environment as they relate to the collection of personal information. This law applies to any website targeted to children under the age of thirteen and requires parental permission for the collection, use or disclosure of any personal information from this group. Additionally, it is noteworthy from a compliance standpoint that the law also applies if the website operator has actual knowledge that it is collecting personal information from a child. As a result of industry pressure and a desire to avoid the passage of overly restrictive legislation, many if not most companies operating a website have adopted and posted on their site a privacy policy outlining data collection and use practices. While generally accepted as a good business practice for any website business, the posting of a privacy policy

[5] Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[6] 15 U.S.C. §§ 6501-06 (1998).

can be the source of a Section 5 cause of action under the FTC Act (i.e., an unfair or deceptive act or practice in or affecting commerce) if the company violates its own privacy policy. The Federal Trade Commission ("**FTC**") can seek injunctive remedies and bring civil actions. Before posting the policy, it is critical to conduct the due diligence necessary to identify and understand actual company technical and marketing practices regarding the collection and use of data so that those practices will be accurately reflected in the posted policy. There is no 'one size fits all' privacy policy for websites and companies that cut and paste their policies from other websites without sufficient internal inquiry may be incurring significant risk. FTC Act authority in regulating privacy is discussed in greater detail below.

Contrary to the market approach to privacy historically followed by the United States, the European Union issued a very specific and comprehensive Data Protection Directive in 1996 (the "**EU Data Directive**"), highlighting the fundamental importance it places on an individual's right of privacy. The EU Data Directive provides protection of personal information maintained by a broad range of companies across different industries and restricts the flow of personal data outside the EU in an attempt to ensure an adequate level of protection outside EU borders. The Safe Harbor Arrangement between the EU and the United States, established in 2000, permits U.S. companies to voluntarily comply with certain principles (e.g., notification, access/correction, limitations on use without consent, reliability and protection from misuse) that are agreed to constitute the required adequate level of protection. Compliance and enforcement falls under the FTC and DOT.

On the government side, the Federal Privacy Act of 1974[7] ("**Privacy Act**") was designed to address privacy issues in connection with the records of federal government executive and regulatory agencies, requiring agencies to apply basic fair information practices to records containing individual personal information. In addition to regulating the collection and use of records by federal agencies, the Privacy Act affords individuals the right to access and correct their personal information. In partial response to the "routine use" exception in the Privacy Act allowing agencies to disclose the data for "routine use" so long as such use was compatible with the original purpose of its collection, The Privacy Act was amended by the Computer Matching & Privacy Protection Act of 1988 and amendments thereto in 1990[8] (the "**Matching Amendments**") to establish requirements that federal agencies must follow when matching information on individuals with information held by other agencies. Obviously, such matching can create powerful and valuable data profiles on individuals. Additionally, there is the Electronic Communications Privacy Act of 1986[9] ("**ECPA**"), amending the federal wiretap law to extend coverage to specific types of electronic communications such as email, cell phones, and computer transmission, extending the ban on interception to the communications of wire or electronic communication services, and restricting access to stored wire and electronic communications and transaction records. The USA-PATRIOT Act of 2001 ("**Patriot Act**") made several significant changes to ECPA, granting the government additional rights with respect to the collection of and access to electronic communications with a focus on governmental security interests.

[7] 5 U.S.C. § 552a.
[8] 5 U.S.C. § 552a (a)(8)–(13), (e)(12), (o)-(r), (u).
[9] 18 U.S.C. §§ 2570-2522, 2701-2711, 3121-3127.

D. Understanding the Origin

Based on the specifics and limited applicability of these federal privacy laws, it is not surprising that many companies have concluded that their respective businesses and industries are not subject to federal privacy laws and, therefore, they are not at risk for data breaches or noncompliance issues. However, a review and understanding of the origin of these laws as well as the broad authority granted to the FTC, coupled with a review of current and expected business trends may suggest that the inquiry should go further. As mentioned briefly above, the FTC has been active in pursuing claims against companies who violate their posted privacy policies in reliance on the FTC Act[10] prohibition against unfair or deceptive acts or practices affecting commerce. Although it is unclear as to whether a privacy policy is required under the Act (i.e., whether it is an unfair or deceptive practice to fail to give consumers notice of potential uses at the time of collection), if a company elects to post such a policy, the FTC reasons that that such a policy is effectively a promise or commitment to consumers. The FTC's authority extends to injunctive relief as well as civil actions. Importantly, each state has adopted its own consumer protection laws, most of which, at a minimum, track the FTC requirements. Again, while some question remains as to whether the law requires a company to post a privacy policy on a site that collects data, the general practice is to post such a policy and the benefits of posting a carefully drafted policy may outweigh any negative risk. To preserve operational flexibility, most policies include a clear statement reserving the right to modify the policy from time to time. Of course, it is critical to periodically review a privacy policy to ensure that it stays current with actual business practices.

With respect to the impetus behind these laws, whether looking at the laws targeted to the private sector or those targeted to governmental agencies, it is fairly easy to identify certain key marketplace developments that prompted new privacy concerns. Such developments include technology innovation and proliferation, the existence of large databases of personal information, an increased public awareness of data collection and use practices and the related security risks, tension between security and privacy interests, and use of an individual's social security number as a general identifier well beyond its initial intended purpose of use in connection with the Social Security system. Arguably, any significant change in transacting business or consumer behavior that would increase the flow and collection of personal information data could be expected to prompt new concerns and possible legislation (e.g., IT/BPO outsourcing, digital rights management, RFID, GPS-based services, and electronic commerce). While historical privacy concerns have focused largely on the damage that may be caused by misuse of personal information, current proposals to regulate the collection and use of personal data also implicitly recognize the value associated with such data. This trend can be expected to continue as future laws will likely seek to recognize and preserve the value of the data to and for the individual while simultaneously minimizing the risk of any unauthorized access and harmful misuse.

As communications technologies evolve and converge and businesses rely more on these new technologies, including the Internet, to transact business and computerized systems are put into place, particularly those that rely in part on the Internet, to manage their

[10] 15 U.S.C. § 45.

customer and employee information, we can, in fact, see the same factors come into play that drove the perceived need for earlier laws. The need for data and highly sophisticated systems to manage that data is no longer limited to financial institutions, data brokers, and health organizations, but rather extends to a broader array of businesses and industries looking for ways to take advantage of new communication methods and devices to reach an increasingly mobile group of consumers. Companies want and need to understand the needs and preferences of their customers so they can personalize services and benefits to create competitive advantages. Targeted messaging has generally been shown to result in higher conversion rates from prospects to customers. This is evident in recent trends around data mining and related matching processes designed to generate consumer profiles with commercial value to the business owner. From a legal compliance perspective, we can anticipate the passage of laws protecting the collection, use, storage and disposal of personally identifiable information. At a minimum, it is likely that these laws will be premised on some type of consent/authorization approach with consumers retaining significant control over their data. From a business perspective, the value associated with this data should encourage the adoption of business practices that promote consumer trust and, in turn, disclosure and usage rights, and put in place data security protections designed to protect such data in a manner at least as protective as those procedures applicable to the company's existing trade secrets. As discussed in greater detail below, the focus should be on mitigation of risk, compliance (i.e., implementation of internal and external controls and security), and crisis management.

E. Information Privacy and Identity Theft

The FTC reports that, on average, victims of identity theft spend five hundred dollars "to deal with their identity theft experience," thus bringing the total annual consumer cost of identity theft to approximately five billion dollars.[11] Adding to the direct financial costs to victims is the considerable amount of time they must spend in order to resolve all of the related problems caused by the fraud committed in their names. The FTC estimates that victims spent an average of 30-60 hours resolving the problem, suggesting that Americans spent over 300 million hours to address and clear up the mess that someone else made of their names.[12] One study estimated the total cost to business and victims in connection with identity theft as $56.6 billion in 2005.[13] In response, recent legislation and business practices attempting to curb invasive practices are becoming increasingly relevant to a broader range of companies, with a focus on security.

The Fair and Accurate Credit Transactions Act ("**FACTA**") was passed in 2003 (amending FCRA) and designed to provide some protection against identity theft. Pursuant to FACTA, consumers may place fraud alerts in their credit files, consumers are entitled to receive notice of credit file data that adversely impacts their receipt of credit, credit and debit card numbers must be truncated on receipts, and credit reporting agencies must provide free annual credit reports to consumers upon request. Through FACTA, Congress pre-empted the

[11] Fed. Trade Comm'n, Identity Theft Survey Report 4 (Sept. 2003), at http://www.ftc.gov/os/2003/09/synovatereport.pdf (last visited July 13, 2006) [*hereinafter*, Survey Report]. Two of the purposes of this study were to "estimate the incidence of Identity Theft Victimization" and to "measure the impacts of Identity Theft on the victims." Data was collected by TeleNation, Synovate's omnibus survey, by conducting over 4,000 telephone interviews of a random sample of U.S. adults over the age of 18 between March 17, 2003, and April 23, 2003. Id. at 6-7.

[12] *Id*.

[13] 2005 BBB/Javelin Survey.

states on credit and debit card transactions to set a national standard (i.e., only last 5 digits of a card number may appear on electronically printed receipts). Since that time, data privacy and data security have continued to be the focus of much media attention due to concerns over identity theft. Much of this attention has been the result of high-profile security breaches related to personal information. These breaches have been the result of internal problems (e.g., employee theft, error or improper use of data) and external problems (e.g., fraud, theft or error). They have also involved tangible formats containing data (e.g., Time Warner) and electronic formats containing data (e.g., ChoicePoint). In any event, the implementation of strategic controls designed to protect and secure the sensitive data from internal and external threats is critical.

Why the flurry of security breaches? Perhaps it is ease of access given its electronic form; maybe it is the intrinsic and commercial value of the data, which is maximized by the size of today's databases and frequency of electronic data transfers; maybe it is the anonymity associated with transacting over the Internet; or, alternatively, maybe it is some combination of these and other factors. The fact remains that these breaches have resulted in significant media coverage and a flurry of activity in Congress in the form of various information privacy bills proposed in both the House and Senate. Additionally, because the existing federal laws and regulations provide for a somewhat piecemeal protection of technological privacy, many states have enacted legislation to fill in the gaps. As will be discussed in greater detail below, the most aggressive state has been California, with the enactment of such laws as the California Computer Security Breach Act,[14] California Financial Information Privacy Act,[15] Disclosure to Direct Marketers Law,[16] California Online Privacy Protection Act, and the Personal Information Security Law.[17]

Increasingly, U.S. laws and regulations attempting to prevent the technological invasion of privacy are aimed at security breaches within a company's collected database. This approach differs from the EU Data Directive in approach which focuses more on the privacy rights of the individual. To this end, two trends have emerged in the U.S.: prevention (i.e., security) and mitigation (i.e., notification). Specifically, the trend in U.S. privacy law is the requirement that companies engage in an ongoing and repetitive process designed to assess risks, as well as identify and implement appropriate security measures as a means of prevention. While the specific measures are generally left up to the company, the measures must be responsive to the particular threats facing the company. California led the way in data notification statutes with its passage of California S.B. 138, effective in July 2003. Recognizing the costs and risks associated with identity theft and the critical role of security in protecting information privacy, this law was intended to give individuals early notice when the confidentiality of any computerized data that includes their personal information was compromised by unauthorized access. As a result, companies in control of the data are encouraged to implement appropriate security safeguards to protect the information and consumers are simultaneously afforded an opportunity to take timely actions designed to protect their identities and mitigate damages resulting from identity theft.

[14] California Computer Security Breach Act, SB. 1386 (2002).

[15] California Financial Information Privacy Act, SB. 1 (2004).
[16] Disclosure to Direct Marketers Law, SB. 27 (2002).
[17] Personal Information Security Law, AB. 1950 (2004).

Several states have followed California in adopting data notification statutes. Legislation has been enacted in at least thirty-four states[18] and proposed in all but four of the remaining states[19] as of this writing. Many of the data breach notification laws are part of a broader effort to address the security of personal information and identity theft[20] and most follow the provisions included in the California statute. However, while the California statute specifically addresses computerized data containing personal information, other states have extended their respective data breach notification laws to generally cover all personal information data regardless of the form of that data. States also differ on the definition of "personal information," with some states providing a very broad definition of that term beyond driver's license or state identification card number, social security number, date of birth, and financial account number including PIN (in each case combined with name) to include "any equivalent form of identification." A couple of states (e.g., Georgia and Maine) close the gap associated with the name requirement (i.e., reverse look-up capabilities) to cover disclosure of personal information together with the individual's address. While all states address notification in the event of a breach, some states limit the notification to circumstances likely to result in injury or damage to the individual. There are other variances among the state laws in notification procedures and timelines, exemptions for entities covered under certain federal privacy statutes, remedy (i.e., private cause of action or enforcement by attorney general only). Nevada and North Carolina are thought to provide the broadest definitions of personal information, with Nevada expressly including an employer identification number within its definition.[21]

Despite an awareness of the compliance issues created by a multi-state regulatory scheme on data notification, federal data notification legislation has been unsuccessful to date. As indicated above, several bills have been proposed and continue to be proposed but the issue has become a highly politicized one due, in part, to general tension and debate regarding the proper balance between the government's legitimate interest in national security and an individual's right to privacy. While proposals have differed on issues of state preemption and minimum encryption or data redaction requirements that would effectively provide a safe harbor from the law, they generally adopt a process-focused approach in line with the approaches found in other data protection legislation, such as GBL, HIPAA, and the Federal Information Security Management Act (FISMA).[22]

Examples of proposed federal privacy legislation include the Information Protection and Security Act, which would require the FTC to regulate all "information brokers." The definition of "information brokers" is so broad that virtually any business that maintains or processes personally identifiable data will be subject to the regulations, although this impact is contrary to the stated intent. In an effort to protect the privacy of consumer information and reduce the risk of fraud and identity theft, the FTC promulgated the Disposal Rule.[23] The new rule requires businesses and individuals who use a consumer report for a business purpose to take appropriate measures to dispose of sensitive information derived from

[18] Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, Washington and Wisconsin.
[19] Mississippi, New Mexico, South Dakota and Wyoming.
[20] Broader legislation may include: (i) legislation criminalizing identity theft; (ii) credit freeze legislation; (iii) legislation addressing use of social security number as a form of identification; and (iv) legislation giving the customer certain access and other rights with respect to credit reporting information.
[21] Nevada Revised Statute 205.4617.
[22] 44 U.S.C. § 3544(b).
[23] FTC, Bus. Alert (June 2005), at http://www.ftc.gov/bcp/conline/pubs/alerts/disposalarlrt.htm (Last visited July 18, 2006).

consumer reports or records to protect against "unauthorized access to or use of the information."[24] The Identity Theft Protection Act,[25] passed by the Senate Commerce, Science, and Transportation Committee, would require companies to notify consumers when their personal information is compromised and there is a "reasonable risk of identify theft."[26] This bill is more consistent with historical privacy laws limiting protection to circumstances where there is potential harm, contrary to the California "any security breach" approach. In addition, the Identity Theft Prevention Act of 2005 attempts to protect the integrity and confidentiality of a person's social security number by prohibiting the Federal Government from mandating the use of a social security number or any other identifying number, except for terrorist or law enforcement purposes.[27] Effectively, it would create a new property right for individuals, recognizing both the privacy interests and inherent value in a social security number. Under the Act, the social security account number issued to any individual would be the exclusive property of such individual.[28]

Other proposed legislation issues include who should have enforcement authority and whether state or agency regulation is more appropriate. The proposed Notification of Risk to Personal Data Act,[29] passed by the Senate Judiciary committee, answers this question by providing for legal action by state attorney generals.[30] The bill would require any person or entity that owns or licenses computerized data containing sensitive personal information to (1) implement and maintain reasonable security and notification procedures and practices to protect sensitive personal information from unauthorized access, destruction, use, modification, or disclosure; and (2) notify any U.S. resident whose sensitive personal information was compromised.[31] The Personal Data Privacy and Security Act of 2005,[32] also provides for legal action by state attorneys general. The bill would require the government to establish rules protecting privacy and security when it uses data broker information and to impose penalties on government contractors that fail to comply.

The Privacy Act of 2005 would prohibit the sale, display, or purchase of social security numbers and other personally identifiable information, subject to a safe harbor, without the individual's consent.[33] Also the Online Privacy Protection Act of 2005 would make it unlawful for an operator of a website or online service to collect, use, or disclose personal information in a manner that violates FTC regulations, subject to disclosures in good faith pursuant to safe harbor regulations to be issued by the FTC.[34] Additionally, the Consumer Privacy Protection Act of 2005 would establish certain rules on privacy notices to consumers, including privacy policy statements.[35] Consumers would have the opportunity to limit sale or disclosure of information and to limit other information practices. Data custodians would have certain statutory information security obligations. For compliance,

[24] *Id.*
[25] S. 1408 (2005).
[26] *Id.*
[27] Identity Theft Prevention Act, H.R. 220, 109th Cong. § 2(c) (ii) (2005), to amend Title II of the Social Security Act and the Internal Revenue Code of 1986.
[28] *Id.* at § 1(c) (ii) (2005).
[29] S. 1326 (2005).
[30] *Id.*
[31] *Id.*
[32] Pers. Data Privacy and Sec. Act, S.1789, 109th Cong. (2005).
[33] Privacy Act, S. 116, 109th Cong. (2005).
[34] Online Privacy Prot. Act, H.R 84, 109th Cong. (2005).
[35] Consumer Privacy Prot. Act, H.R 1263, 109th Cong. (2005).

there would be self-regulatory programs and other enforcement, but no private right of action.[36]

Notwithstanding the lack of any federal data notification law at present, there is some guidance available on a "best practices" approach. Through a series of settlements, the FTC has effectively adopted national data security standards for companies covered by the FTC Act. In each of these cases, the FTC instituted an action against a company as an "unfair practice" on the theory that they did not do enough in terms of implementing minimal security protections in an effort to prevent the resulting data breach. These de facto standards include some level of data encryption, minimizing risk by limiting storage time to match need, application of meaningful (i.e., non-default) user IDs and passwords, application of readily available security measures to prevent unauthorized wireless connections to the network containing the data, and application of reasonable measures designed to detect unauthorized access to its network and adoption of appropriate security measures.

Many people continue believe a national privacy standard is important to simultaneously protect consumers and remove potential threats to the integrity and growth of electronic commerce and other data-driven products and services. Indeed, it would appear that FTC enforcement actions and penalties are ineffective as a prevention mechanism and as a means for defining optimal security and privacy standards and some type of national standards may be required and, in fact, useful to national businesses. Given California's prominent position regarding privacy law, a focus on California's laws may be appropriate as a starting point. Recommended practices for providing notice of security breaches involving personal information have been prepared by the Consumer Affairs Department for the State of California and are available on the Internet.[37] At a minimum, it would seem that a comprehensive information security program would require companies to: (1) conduct periodic risk assessments to identify the specific threats and vulnerabilities the company faces; (2) define and categorize by sensitivity all information it collects; (3) identify all uses of the information it collects and ensure that customers and employees are informed about such uses; (4) develop and implement a security program reasonably designed to manage and control the risks identified; (5) monitor and test the program to ensure that the security program is effective; (6) continually review and adjust the program in light of ongoing changes; (7) obtain regular independent audits and reports; (8) oversee third party service provider arrangements and retain appropriate audit rights and controls; (9) establish data retention policies reasonably designed to match data needs; (10) define a secure data destruction methodology; (11) establish procedures for data notification and problem resolution; and (12) make senior management responsible for the security program (i.e., CEO, board of directors). Importantly, each of the foregoing components should be considered in the context of both internal and external threats.

F. Spam

New forms of unsolicited advertising and marketing have evolved with each new method of communication, including telephone, television, and, more recently, the Internet. Unsolicited commercial e-mail, or "spam," has gained popularity because it is relatively

[36] *Id.*

[37] *Recommended Practices on Notice of Security Breach Involving Personal Information*, State of California Department of Consumer Affairs at http://www.privacy.ca.gov/recommendations/secbreach.pdf.

cheap, anonymous and hard to track, and effective. It has been estimated that only one person out of 10,000 must respond for a spammer to make a profit. These odds may explain why 2006 statistics show that 12.4 billion spam e-mails are sent each day, a total that represents forty percent of all e-mail. In response to such a high volume of frequently unwelcome e-mail, approximately thirty-seven states have some type of anti-spam legislation. In a 2003 effort to promulgate a comprehensive anti-spam structure, Congress passed and President Bush signed into law, the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act").[38] Since the Act took effect on January 1, 2004, there is conflicting data as to whether the measures have been effective in limiting this practice. Many critics view the CAN-SPAM Act as a watered-down version of the more aggressive legislation enacted in some states, including California, which the Act now pre-empts.

The CAN-SPAM Act explicitly distinguishes between "commercial" messages and "transactional or relationship" messages, and applies only to "commercial" e-mail.[39] Drawing this distinction requires an inquiry into the "primary purpose" of the e-mail. FTC-specified guidelines determine whether the content of an e-mail is primarily commercial, and thus subject to the CAN-SPAM Act, or whether it falls within the "transactional or relationship" exception. An e-mail may be reasonably considered to be a "transactional or relationship" message when the subject matter relates predominantly to an established transaction or relationship previously agreed to by the recipient and arguably continues communication on the same subject between the parties. Examples include messages about the delivery of goods or services, warranty information on a product purchased by the recipient, account information on a subscription, information regarding an employment benefit plan, and information generally of interest to a consumer regarding a past purchase or otherwise necessary to allow a company to fulfill its obligations.

The main provisions of the CAN-SPAM Act include:[40] (1) a ban on false or misleading headers (including from, to, and routing information);[41] (2) the prohibition of deceptive subject lines; (3) the requirement that commercial e-mails give recipients clear and conspicuous notice of an "opt-out"[42] method to avoid receiving such e-mails in the future, as well as a requirement that spammers honor these requests within ten business days; (4) the requirement that commercial e-mail be clearly and conspicuously identified as an advertisement; (5) the sender's valid physical postal address must be included in the message.[43]

The Act grants the FTC, federal agencies, and state attorney generals the authority to enforce violations of the bill.[44] While adversely affected Internet Service Providers ("ISP") may bring actions under the Act, other individual actions are not allowed.[45] Cease and desist orders and injunctive relief may be granted in an action to enforce compliance.[46] Some

[38] 15 U.S.C. §§ 7701 *et seq.*
[39] 15 U.S.C. §§ 7701 *et seq.*
[40] 15 U.S.C. §§ 7701 *et seq.*
[41] Notably, despite the Act's distinction between commercial e-mail and transactional or relationship messages, the provision banning a misleading header applies to both categories.
[42] "Opt-out" refers to a method by which e-mail recipients may indicate that they wish not to receive or not to continue to receive future e-mails.
[43] According to a Federal Trade Commission's *Proposed Rulemaking and Request for Public Comment*, (May 12, 2005), a valid physical postal address includes post office boxes and private mailboxes duly registered with the United States Postal Service. *See* http://www.ftc.gov/os/2005/05/05canspamregformfrn.pdf at 15.
[44] 15 U.S.C. §§ 7701 *et seq.*
[45] *Id.*
[46] *Id.*

actions involving fraud or sexually oriented materials may result in damages or even imprisonment.[47]

Although the CAN-SPAM Act is pre-emptive, some related state laws may still apply, and should be recognized in order to comply fully with spam legislation. Notably, unfair, false or deceptive practices involving commercial spam can still be reached under state anti-spam laws and other laws generally designed as consumer protection laws. Specifically, as discussed earlier, many states have laws that ban false or misleading subject lines, false routing information, and use of false third-party return addresses or domain names that are not pre-empted by CAN-SPAM because they apply to commercial e- mail "or *information attached thereto*." Approximately thirty-two states ban at least one of these practices and twenty states ban all three. Other state laws that are not pre-empted include bans on selling software that can be used to falsify routing information[48] and on violating ISP policies.[49]

As suggested earlier, many people attribute the inability of CAN-SPAM to effectively stop spam in any meaningful way to the perceived dilution of certain state laws. For example, the California counterpart of the "opt-out" provision in CAN-SPAM provided for an "opt-in" requirement that would have prohibited commercial e-mail except when the recipient explicitly consented. So what does this mean for businesses with inboxes full of spam? Unfortunately, the current practical answer appears to be technological rather than legal, suggesting the need to implement strong software programs and filters to minimize interruption to business and protect privacy interests. Experts recommend that businesses get

[47] *Id*.
[48] *Id* at 365. Such legislation enacted in fifteen states.
[49] Such legislation enacted in nine states.

effective spam filters for their computers, or risk the foregone productivity of employee hours spent sifting through bulk mail. Of course the problem with a technology-based solution is the inevitable ability to identify to workarounds.

CAN-SPAM also affects companies on the sending end of commercial e-mail, and the Act can be a trap for unwitting companies, especially those that utilize third party spam marketing campaigns. In the event of a violation, a mitigating factor in the assessment of damages is a review of whether the violation occurred because of or in spite of established and implemented commercially reasonable efforts to prevent such violations.[50]

G. Spyware

Spyware is commonly understood to mean any software that covertly gathers user information through a user's Internet connection often for advertising or other commercial purposes. Spyware applications are often bundled with other consumer applications such as freeware and shareware (e.g., peer-to-peer) and, therefore, operates similar to a Trojan horse. Spyware can monitor key strokes, scan files contained on a hard drive, read cookies, install other spyware programs and even change the default home page on a browser. As such, spyware presents a significant threat to privacy, exposing sensitive private information that is stored on computers, such as credit card numbers, e-mail addresses, passwords, and web pages viewed. As to the latter, spyware effectively provides valuable insight into the host's viewing and buying behavior providing access to a different, but equally personal, type of personal data. The spyware constantly relays private personal information back to the

[50] 15 U.S.C. §§ 7706(f)(3)(D), (g)(3)(D)

program's author. In addition to invading the host's privacy, spyware threatens the host's system security and control and adversely impacts the host's processing abilities by using significant memory and bandwidth.

The Anti-Phishing Act of 2005 would establish a federal crime of "internet fraud" for using another's website address, website, or domain name to induce, request, ask, or solicit any person to transmit, submit, or provide any means of identification to another person.[51] The Social Security Number Protection Act of 2005 would establish new FTC regulations for "information brokers." Individuals have the right to obtain disclosure of all personally identifiable information pertaining to the individual held by an information broker, and to be informed of the identity of each entity that procured any personally identifiable information from the broker.[52] Along similar lines, the Wireless 411 Privacy Act has not passed through the Senate yet, but if enacted, it would affect customer relationship management and call centers by requiring wireless telecommunications carriers to make available a "do not contact my wireless device" (hand-held telephone) rule.[53]

At the state level, the general consensus among the states that have chosen to legislate on the issue of spyware is that if there has been a breach and the personal information is not encrypted, then it is the legal duty of the business breached to inform the victims of the breach if there is a reasonable likelihood of harm. Spyware legislation was enacted in California and Utah in 2004 and was introduced in at least five other states in 2004.[54] In 2005, the number of states introducing legislation grew to 28, and seven states—Arizona, Arkansas, Georgia, Iowa, Utah, Virginia and Washington—enacted legislation so far this year.[55] Many states[56] have adopted the approach of prohibiting, rather than regulating, spyware. California, Arkansas, Georgia, Iowa, Missouri, Nebraska, Texas, and West Virginia have included or are considering including language that would make the use of spyware a criminal offense with liability up to $1,000 per offense. This last set of states has chosen not to prohibit spyware entirely, but rather to regulate the use and limit the access businesses have to consumer computers.[57]

H. Conclusion

Spam, spyware, and security breaches of personally identifiable information are proving to be costly problems with severe consequences that can be staggering for both individuals and businesses. Businesses should seek to adopt a "best practices" approach to data collection, storage, security and use in an effort to protect their customers (and employees) and simultaneously gain customer trust in an effort to position themselves to use this valuable data to develop and target new products and services to interested customers. Issues of data integrity and usage rights should be of critical importance to every company. To protect against spyware and malicious hacking techniques, companies may want to

[51] Anti-Phishing Act, H.R. 1099, 109th Cong. (2005), at http:// thomas.loc. gov/cgi-bin/query/z?c109:H.R. 1099: (last viewed on July 12, 2006).
[52] Fed. Trade Comm'n, *FTC Facts for Business* (May 2006), at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus66.pdf (last visited July 18, 2006).
[53] Wireless 411, S.1305, 109th Cong. (2005), at http:// thomas.loc. gov/cgi-bin/query/z?c109S.1350: (last viewed on July 12, 2006).
[54] 2004 State Legis. Relating to Internet Spyware or Adware (Jan. 28, 2005), at http://www.ncsl.org/programs/lis/spyware04.htm (last viewed July 17, 2006).
[55] 2005 State Legis. Relating to Internet Spyware or Adware (Dec. 27, 2005), at http:www.ncsl.org/programs/lis/spyware05.htm (last viewed July 17, 2006).
[56] Alabama, Alaska, Arizona, Delaware, Florida, Illinois, Indiana, Kansas, Maryland, Massachusetts, Michigan, New Hampshire, New York, Oregon, Pennsylvania, Rhode Island, Tennessee, Utah, Virginia, Washington
[57] *Id.*

consider the merits of limiting employee access to the Internet, much in the same way they currently do via password protection with respect to sensitive software applications and databases, but through the adoption of some type of permissioning approach based on business need. Certainly, software should be installed to block unauthorized downloads of non-business critical freeware and shareware on company equipment via the Internet to protect against spyware applications. Use of appropriate filters can help minimize unauthorized and unproductive interruptions. A company should also have guidelines as to appropriate precautions to recognize potentially harmful emails and attachments and a process for reporting suspicious emails. Companies must do their best to stay ahead of (or at least close to) new privacy threats and tactics so they may adjust security measures, filters and blocking software as necessary from time to time. A comprehensive policy directed at data privacy and security must be dynamic and subject to constant review.

Privacy, Spam & Spyware 2006

Section 311 – ACC Annual Meeting

October 23, 2006

DATA GOVERNANCE POLICY

Document Version 1.0

Table of Contents

Data Governance Policy v1.0

Preface

Document Description

The Data Governance Policy identifies all categories of electronic and hardcopy information owned or controlled by the (COMPANY) and is used as a fundamental basis for:

- Making informed decisions about data and systems;
- Executing authority over the management of data;
- Improving and maintaining the quality of data;
- Establishing appropriate security, backup, and retention over data (including granting appropriate access to data);
- Synchronizing policies, organization and technology around data (including establishing compliance measures for subsequent monitoring and auditing).

Target Audience

The Data Governance Policy applies to all COMPANY owned data, its personnel and third-parties including program partners, strategic partner and service providers.

Document Revision History

Table 1: Document Revision History

Version	Date	Author	Description
Draft 1.0	6/23/2005		First draft of document in updated template
Draft 1.1	7/15/05		Updated draft reviewed by COMPANY Information Technology (IT) staff.
Draft 2.0	7/22/05		Updated draft reviewed by Data Privacy team.
Draft 2.1	10/4/05		Updated draft for review by IT Task Force.
Draft 2.2	10/10/05		Name Change & Updated draft for review by COO and senior management.
Draft 2.3	10/19/05		Updated w/comments from Mtg 10/12/05, and subsequent analysis.
Draft 3.0	10/26/05		Update w/comments from Mtg 10/26/05
Final 1.0	11/7/2005		Updated w/comments from Mtg 11/2/05. Policy approved.

US2000 9489721.1

1 Overview

Data governance is the synchronization of policies, standards, procedures, organization, and technology to help drive increased value from information. A strong data governance program should address each of the items listed below:

- Policies (e.g., data use and other Council policies)
- Standards (e.g., data quality)
- Procedures (based upon enterprise-wide standards)
- Authority (e.g., mandates set by senior management)
- Organizational Structure (e.g., Senior Management – Data Governance Team)
- Roles and Responsibilities (Data Owner, Agent, Consumer, and Custodian)
- Monitoring (linked to defined metrics for measuring success in meeting standards)

The Data Governance Policy contains four key components: Roles & Responsibilities, Directives, Data Categories, and Security Classifications. A process is established for the continuous improvement of the Data Governance Policy.

1.1. Objectives

INSERT ORGANIZATION'S MISSION STATEMENT HERE. The overall objectives of the Data Governance Policy are to support the Organization's mission through the establishment of policies that:

1. Provide a standardized format for identifying and classifying all data and information to which COMPANY personnel, vendors, partners, and other external entities have access.
2. Establish common definitions for how we describe the components of Data Governance, i.e., roles and responsibilities and documentation standards.
3. Define key data categories and sub-categories that support COMPANY operations.
4. Define key data governance roles and responsibilities and assign them to senior management team members and/or other staff.
5. Define the security classification associated with each information class for the purposes of applying the necessary security controls to protect data from threats—internal or external, deliberate or accidental.

Data Governance Policy v1.0

1.2. Key Terms and Definitions

1. **Data**: Factual information (such as measures, responses, or statistics), including without limitation information in numerical form that can be digitally transmitted or processed, that is collected and organized for analysis, to reason, or to make decisions
2. **Data Elements:** Individual components of data.
3. **Dataset:** A collection of data elements stored as an extract or in a common repository.
4. **Data Use Policy:** A policy created for each Data Category for the purpose of applying Council policies to that specific class of information. Data Use Policies include the following:
   - A current mapping of the data (where it resides and flows throughout COMPANY)
   - Business rules for granting access
   - Measures to ensure quality and integrity of the data
   - Data retention rules identified through business needs and legal compliance
   - Internal controls (e.g., security, privacy, contractual terms, etc.)
   - Metrics for measuring quality, compliance, and security
5. **Information:** Data when it is used or transformed for analysis, to reason, to make decisions, or for a specific purpose.
6. **Data Category:** A grouping of data that has common attributes for security, access, retention and compliance requirements

1.3 Glossary of Functions Impacting Data Governance

1. **Enterprise Risk Management Role or Team**: provides input into the Data Governance initiative related to risks that impact specific data policies around use, security, retention, availability, etc.
2. **Information Technology (IT)**: establishes enterprise IT or security policies that must be addressed and provides input into Data Use Policies.
3. **Project Management Office:** manages the Data Governance initiative as a project for initial setup, and assists Owners in developing and updating standards, maintaining an enterprise document storage area for all Data Governance documentation obligations, and ensuring that the continuous improvement and maintenance processes are established.
4. **Legal:** ensures corporate policies and guidance around data retention, privacy, vendor management, and other compliance initiatives are fed into the Data Governance framework.
5. **Senior Management Team:** serves in the role of the Data Governance Team in creating and evolving the existing framework to meet changing business needs and evaluating new data or material changes to data.

US2000 9489721.1

1.4 Governance Directives

The following directives govern and enforce data standards, stewardship, procedures, and controls put in place by COMPANY.

1. **Data is the property and a key asset of COMPANY. Senior management serves as the Data Governance Team and is responsible for setting overall policies regarding these assets.** Individual members of senior management have defined ownership roles over specific assets. All employees must recognize that the proper management of data is critical to the success of the organization.
2. **Individuals recognized as Owners, Agents, Consumers (primary and secondary), and Custodians of data are designated by the Data Governance Team**. All roles have specific accountabilities related to data management incorporated into their job descriptions.
3. **All data is mapped, named, and defined across the business functions of COMPANY using common documentation standards.** PMO and Information Technology assists Owners in developing and updating standards, maintaining an enterprise document storage area for all data governance documentation obligations, and ensuring that the continuous improvement and maintenance processes are established.
4. **Data is accessible to those who need it in order to perform an essential role in their job function, within appropriate security classification restrictions.** Every effort must be made by management to share data across functions and reduce redundant data. When restrictions are made (e.g., by regulations or policies), Owners of the data are accountable for defining specific individuals and levels of access privileges that are to be enabled through security access controls. Ongoing monitoring of compliance is commensurate with the value of the data and it's security classification and reported back to the Data Governance Team.
5. **The needs of Agents, Consumers, and Custodians are considered and incorporated into the design and modification of data processes (both upstream and downstream), procedures, and standards.** Owners should seek input from all stakeholders when making key decisions around data.
6. **Data quality shall be improved, maintained, and measured to ensure users can rely on the accuracy and integrity of data and its sources.** The results from measuring data quality should be continuously fed back into the data governance process.
7. **Data in all formats shall be safeguarded and secured based on recorded and approved corporate policies, requirements and compliance guidelines.** These requirements are directed at a policy level by Owners. Appropriate technical, physical, and administrative controls are implemented to safeguard information based on its security classification scheme.
8. **A Data Use Policy shall be created for each Data Category for the purpose of applying corporate policies to that specific class of information.**
9. **The Data Governance Team will ensure that COMPANY implements appropriate training on data governance and data use policies.**

The following Data Governance roles and responsibilities shall be assigned to each data category. While one Owner is designated for each Data Category, multiple Agents, Consumers, or Custodians may exist across COMPANY.

KEY: RACI Roles: R = Responsible; A = Ultimate Authority; C = Consult; I = Inform

Data Governance Policy v1.0

Table 2: Data Governance Roles and Responsibilities Table

Role	Definition
Owner (A)	Individual with decision making authority who is responsible for providing strategic direction and policy guidance around a Data Category in both upstream and downstream processes, including: • Integration, quality, and integrity • Availability and retention • Methods to ensure compliance and data use (including when data is transformed into information as defined by this policy) • Security, administration, and access • Measurement, monitoring, and enforcement
Agent (R)	Function(s) responsible for ensuring that data is created, updated, or maintained, and are accountable as delegated by Owners for: • the quality and integrity of data that is produced or gathered from sources • applying compliance rules regarding collecting or creating data • adhering to security and access controls placed around data
Consumer (1) Primary (C) (2) Secondary (C or I)	Any function (COMPANY personnel, vendor, service provider, etc.) who utilizes data from a COMPANY system that is responsible for compliance regarding data use, security and access controls. Consumers are defined in primary and secondary categories. A **Primary Consumer** is on the critical path of the data lifecycle and affected by upstream data decisions. They are heavily reliant on Agents for the quality of the data and need to be consulted on key decisions regarding data. They are also likely a key source of data for Secondary Consumers and may have some Agent responsibilities for downstream data use. A **Secondary Consumer** is not on the critical path for the data lifecycle and is affected by downstream data decisions. Data use by Secondary Consumers is periodic, and the data may generally be used in a de-identified or aggregate form. Secondary Consumers need to be informed of upstream data decisions.
Custodian (R)	COMPANY personnel responsible for building and maintaining the infrastructure used to support data production and consumption, and are accountable for ensuring systems tactically accommodate policies concerning data: • Availability and retention (backup) • Security, administration, and access • Enables tools for quality assurance, measurement, monitoring, and enforcement

The following are the Data Categories used to define common data sub-categories and elements and

US2000 9489721.1

attributes that govern the security, access, retention, back-up, design of business requirements and corresponding policies and procedures.

Table 3: COMPANY Data Categories

CATEGORY	DESCRIPTION
Financial Data	
Customer Data	
Human Resources Data	
Information Technology	
Research/Patents	
Management Data	
Legal Data	

A **Security Classification** is the level of sensitivity that defines how data categories are protected and secured from threats. All data and information assets across COMPANY are classified according to the following table. Each classification applies to all of the data categories listed in previous sections. These security classifications will be aligned with those of key vendors as required.

Table 4: Security Classifications Table

Classification	Definition
Super Secret	**Data/information of the highest confidentiality, sensitivity and value which, if revealed, could cause direct damage to the finances, operations, or reputation of COMPANY.** • Access to such data is strictly limited, audited, and controlled at all times. New access to such data must be approved by the Data Governance Team. • Once this information is secured, a limited number of individuals are able to view select sections of the data. • The individuals who have access are regularly audited to ensure that the confidentiality of this information is maintained.

Data Governance Policy v1.0

Restricted	**Data/information that requires less stringent controls than "Super Secret" which, if compromised, could have a negative impact on the finances, operations, or reputation of COMPANY.** • Access to such data is limited to the few people within COMPANY who have vested interests in such information and need to know the information to perform their essential job functions.
Confidential	**Data/information with a high sensitivity because of its possible financial, operational, or privacy impact to COMPANY or individuals.** • Information is revealed only to COMPANY personnel who need to know the information to perform their essential job functions.
Internal Use Only	**Data/information that is intended for use within COMPANY only.** • This information is not approved for general circulation outside of COMPANY where its disclosure would inconvenience the organization or its management. Note: A compromise of such data is unlikely to result in financial loss or serious damage to credibility.
Restricted Release	**Data/information for which business restrictions are applied that determine which audiences receive such data/information.** • This data may be required to be protected under trade secret law and thus requires additional security considerations.
Public	**Data/information that is made available to the public or that is published on COMPANY Web sites.** • The disclosure of this information would not expose COMPANY to financial loss or legal risk, impair the effective operations of COMPANY or harm the Company's image.

The Data Governance Policy shall be reviewed annually by the Data Governance Team. This may include performing additional assessments to identify new or additional data, changes in the technology environment or organization. Periodic audits will be conducted to ensure compliance with the Data Governance Policy and the results will be shared with senior management. Senior management will then determine appropriate remediation plans. The Data Governance Team shall ensure that policies and procedures are benchmarked in line with industry trends.

US2000 9489721.1

Data Governance Policy v1.0

The following matrix depicts the roles and responsibilities assigned by the Data Governance Team for each Data Category as of 10/1/2006. The Phase I date is the target deadline for completion of current state and gap analyses for each category, needed as inputs to the Data Use Policy.

Table 5: Roles & Responsibilities by Data Category Table

DATA CATEGORY	DESCRIPTION	OWNER	AGENT	CONSUMER	CUSTODIAN	Phase I Dates
1.Financial Data	Data relating to payment information, transaction details of online purchases, invoices and receipts, accounts receivable and payable records, financial statements, expense reports, Vendor Master File financial information.	CFO	Finance	(1) Finance, Executive Office (1) CS, Budget/ Vendor Managers, Legal	Finance, IT	6/30
2. Customer Data	Data relating to purchasers of COMPANY products	Customer Service	CS	(1) CS, R&D (2) Legal	IT	7/1
3. Human Resource Data	Data relating to COMPANY personnel (including disciplinary and performance data) and staff recruitment.	HR	HR	(1) HR (2) All	HR/IT	TBA
4. Information Technology	Data that the IT Department maintains, has access to, or uses for security purposes and/or systems operations, configuration, and maintenance. It includes technology infrastructure documentation, inventory of software and hardware systems, backup data, log files, error handling modules.	COO	IT	(1) IT (2) All	IT	TBA
5. Research/Patents	Data relating to technology, patents, trade secrets/processes	OPS	Ops	(1) Ops, CS (2) Legal, R&D, Exec Office	IT	TBA

US2000 9489721.1