



Keeping Information Private

May 24, 2011



Introductions – Your Presenters

- Andy Hepburn (hepburn@neolaw.com)
- Kim Verska (verska@fsblegal.com)
- Tammy Moskites (Tammy_Moskites@homedepot.com)



Mission of Pro Bono Partnership of Atlanta:

To provide free legal assistance to community-based nonprofits that serve low-income or disadvantaged individuals. We match eligible organizations with volunteer lawyers from the leading corporations and law firms in Atlanta who can assist nonprofits with their business law matters.

Pro Bono Partnership of Atlanta Eligibility & Other Information

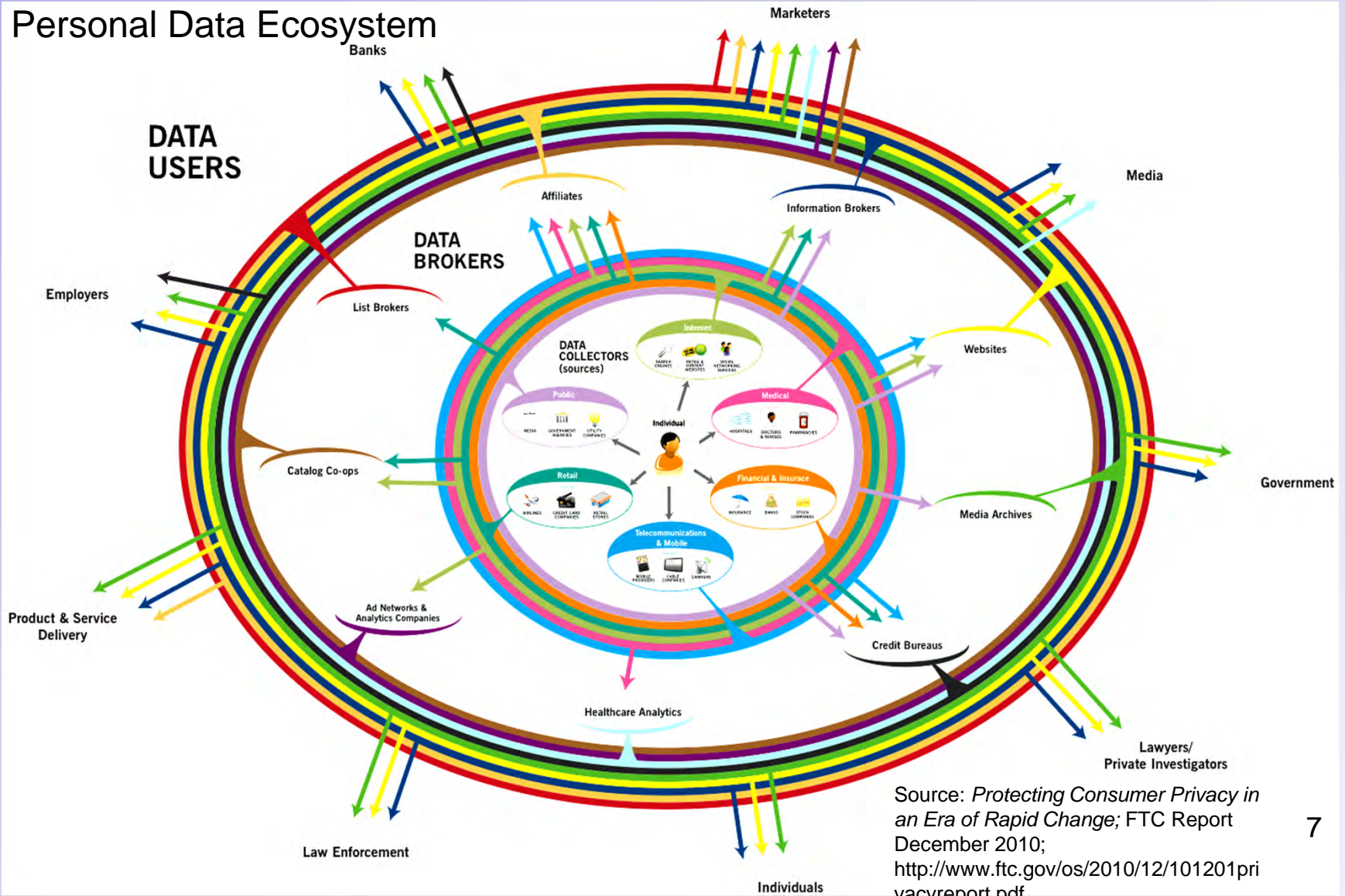
- In order to be a client of Pro Bono Partnership of Atlanta, an organization must:
 - ✓ Be a 501(c)(3) nonprofit organization.
 - ✓ Be located in or serve the greater Atlanta area.
 - ✓ Serve low-income or disadvantaged individuals.
 - ✓ Be unable to afford legal services.
- *Visit us on the web at www.pbpatl.org*
- Host free monthly webinars on legal topics for nonprofits
 - ✓ To view upcoming webinars or workshops, visit the [Workshops Page](#) on our website

- **Anatomy of a Privacy Breach**
- **Risk Assessment**
- **What Do We DO?**
 - ✓ Setting the Bar: “What does The Home Depot do?”
 - ✓ The Current State of the Law
 - ✓ Service Provider Obligations
 - ✓ Practical Compliance Programs
- **Key Components of a Privacy Program**
 - ✓ Privacy Policy
 - ✓ Records Management
 - ✓ Training, Communications, Enforcement, Monitoring
- **The Privacy Policy**
- **Records Management Procedures**
- **Q & A**

➤ **Situation:** Personal information increasingly is the target for criminals and other ne'er-do-wells. It's much easier to hack a network than to rob a bank, and more lucrative, too. As more of our personal information becomes digitized, the risks of it falling into the wrong hands is increasing dramatically.

SCOPE: Who has YOUR personal data?

Personal Data Ecosystem



Source: *Protecting Consumer Privacy in an Era of Rapid Change*; FTC Report December 2010; <http://www.ftc.gov/os/2010/12/101201privacvreport.pdf>

➤ **PROBLEM: Cases in April 2011 alone:**

- ✓ **Sony Playstation Network** hack exposed the personal data of over 77 million customers, including names, email addresses, and maybe credit card numbers
- ✓ **Epsilon** exposed names and emails of the following companies: Target, Kroger, TiVo, US Bank, JPMorgan Chase, Capital One, Citi, Home Shopping Network, Ameriprise Financial, LL Bean Visa Card, McKinsey & Company, Ritz-Carlton Rewards, Marriott Rewards, New York & Company, Brookstone, Walgreens, The College Board, Disney Destinations, and Best Buy have notified their own customers about the breach. Hilton Hotels and Ethan Allen

Sony's nightmare ...



ANATOMY OF A PRIVACY BREACH

First Twitter gets a whiff of trouble...



PlayStation Network down for a long
count, what's up Sony?


<http://engt.co/gn9rFD>

21 Apr via [twitterfeed](#) ☆ [Favorite](#) ↻ [Retweet](#) ↩ [Reply](#)

Then the BLOGS begin to feast...

KOTAKU

Sony Working Around the Clock To Restore Playstation Network and Online Gaming

 **Brian Crecente** — Sony officials continue to work around the clock to bring the downed Playstation Network back online after an "external intrusion" forced the company to take the system down.



Lease a new 2011 Prius
\$299* PER MONTH 36 MONTHS
\$2,298 DUE AT SIGNING
WITH APPROVED CREDIT

Now Includes  ToyotaCare

... and BIG NEWS joins the fray

The New York Times

Bits

Business ■ Innovation ■ Technology ■ Society

MAY 2, 2011, 11:32 PM

Sony Finds More Cases of Hacking of Its Servers


By *NICK BILTON*

Sony said Monday that it had discovered that more credit card information and customer profiles had been compromised during an attack on its servers last week.

In a news release issued by Sony, the company said that it had discovered hackers had gained access to the Sony Online Entertainment servers, which contain approximately 24.6 million customer accounts and 12,700 credit card and debit card numbers. Sony said the hackers might have stolen this information, but the company could not be sure.

Whereupon the law arrives...

FBI Cybercrimes Joins 22 States In Sweeping PlayStation Network Investigation

 **Brian Crecente** — The Federal Bureau of Investigations today confirmed to Kotaku that it is looking into the security breach that brought the Playstation Network down and exposed millions of users' personal data to cybercriminals.

The FBI is joined by nearly two dozen state attorneys general and possibly the Federal Trade Commission who are looking into this month's Playstation Network hack attack which forced Sony to take their PS3 online service offline for more than a week.



Lease a new 2011 Prius

\$299* PER MONTH 36 MONTHS
\$2,298 DUE AT SIGNING
WITH APPROVED CREDIT

Now Includes  Toyota Care

[FIND YOURS TODAY](#)

*details

Eventually, damage control commences ...

```
=====
PlayStation(R)Network| April 26, 2011
=====

Valued PlayStation(R)Network/Qriocity Customer:

We have discovered that between April 17 and April 19, 2011,
certain PlayStation Network and Qriocity service user account
information was compromised in connection with an illegal and
unauthorized intrusion into our network. ...

Although we are still investigating the details of this incident,
we believe that an unauthorized person has obtained the following
information that you provided: name, address (city, state, zip), country,
email address, birthdate, PlayStation Network/Qriocity password and login,
and handle/PSN online ID. ... While there is no evidence at this time that
credit card data was taken, we cannot rule out the possibility. If you have
provided your credit card data through PlayStation Network or Qriocity,
out of an abundance of caution we are advising you that your credit
card number (excluding security code) and expiration date may have
been obtained.
```

And costs to fix the problem skyrocket!

The Christian Science Monitor - CSMonitor.com

Sony data breach could be most expensive ever

Sony Corp.'s PlayStation Network and Sony Online Entertainment suffered data breaches that could cost up to \$2 billion.



2 Billion!

Privacy Breach - What are the risks?

- Harm to reputation
- Loss of income / donor good will
- Loss of staff focus on cause / mission
- Costs of restitution to affected individuals
- Government fines and penalties
- Lawsuits

**Could one privacy breach destroy
your organization?**

SO, WHAT DO WE DO?

Setting the Bar – The Home Depot Approach

IT Compliance & Data Privacy The Home Depot Approach



Tammy Moskites, CISM
Chief Information Security Officer, Information Assurance

How do you get Started?

Protecting ANY business – no matter how big or how small – must be focusing on Security and Privacy – it starts with three critical tasks:

- Assess Your Risks
- Draft and Implement a Security Plan/Program
- Ongoing Monitoring of Threats to Your Business

IT Compliance & Data Privacy Program

- ✓ Created a Data Classification Matrix – define and assign
- ✓ Security Policy, Standards and Guidelines
- ✓ Built an experienced IT Compliance Security Team
- ✓ Map *current* security controls to Regulatory Requirements
- ✓ Perform a Gap Analysis of Controls vs. Regulatory requirements – define *ideal* state
- ✓ Ongoing focus to Enhance and Enforce Security Controls
- ✓ Partner, Partner, Partner

Data Classification – Matrix

#	Type Description	Restricted Information Minimum Handling Requirements	Confidential Information Minimum Handling Requirements	Internal Use Information Minimum Handling Requirements	Public Information Minimum Handling Requirements
1.	By Electronic Messaging (E-Mail)	Sender must confirm receipt of message; message body and all attachments must be encrypted (1)	Message body and all attachments must be encrypted (1)	No special requirements	No special requirements
2.	By FAX	Attended at receiving FAX; Sender must confirm receipt of message	Attended at receiving FAX	Data custodian to define requirements	No special requirements
3.	By Inter-Office Mail	Hand delivery only	No external labeling on envelope; "HOME DEPOT CONFIDENTIAL" labeling on all media or hardcopy	No special requirements	No special requirements
4.	By LAN	Sender must confirm receipt of message; Data must be encrypted (1)	Data or network connection must be encrypted (1)	No special requirements; Encryption optional (1)	No special requirements
5.	By Voice-mail	Confirmation of receipt required (sender); remove message after receipt (recipient)	No special requirements	No special requirements	No special requirements
6.	By Wireless, Cellular Phone (includes text messages), Blackberry SMS and Pagers	Do not transmit or discuss	Do not transmit or discuss	No special requirements	No special requirements
7.	Deleting access to information	Data custodian to authorize individual users in writing; user confirmation required.	Data custodian to authorize individual users; user confirmation required	Data custodian to define permissions on user, group or function basis	Data custodian to define permissions

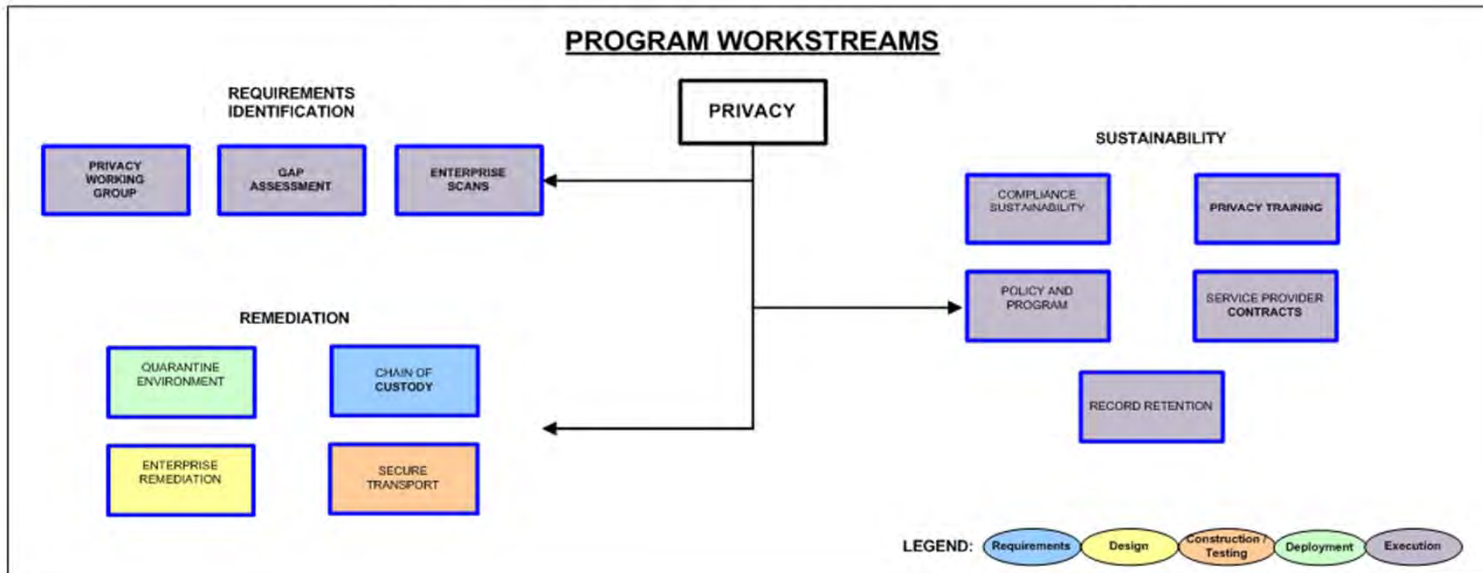
Example



EXAMPLE

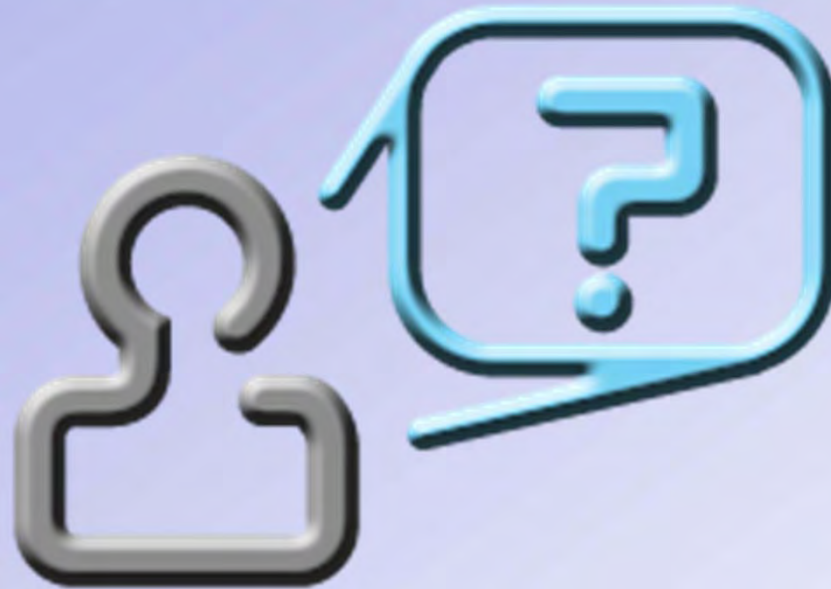
IT Compliance Program 2011

As of: May 10, 2011 1.0



Key Things to Remember

- *Prevention*. Solutions, policies and procedures need to be identified to reduce the risk of attacks.
- *Resolution*. In the event of a computer security breach, plans and procedures need to be in place to determine the resources that will be used to remedy a threat.
- *Restitution*. Companies need to be prepared to address the repercussions of a security threat with their employees and customers to ensure that any loss of trust or business is minimal and short-lived.



Tammy Moskites, CISM
Chief Information Security Officer
The Home Depot

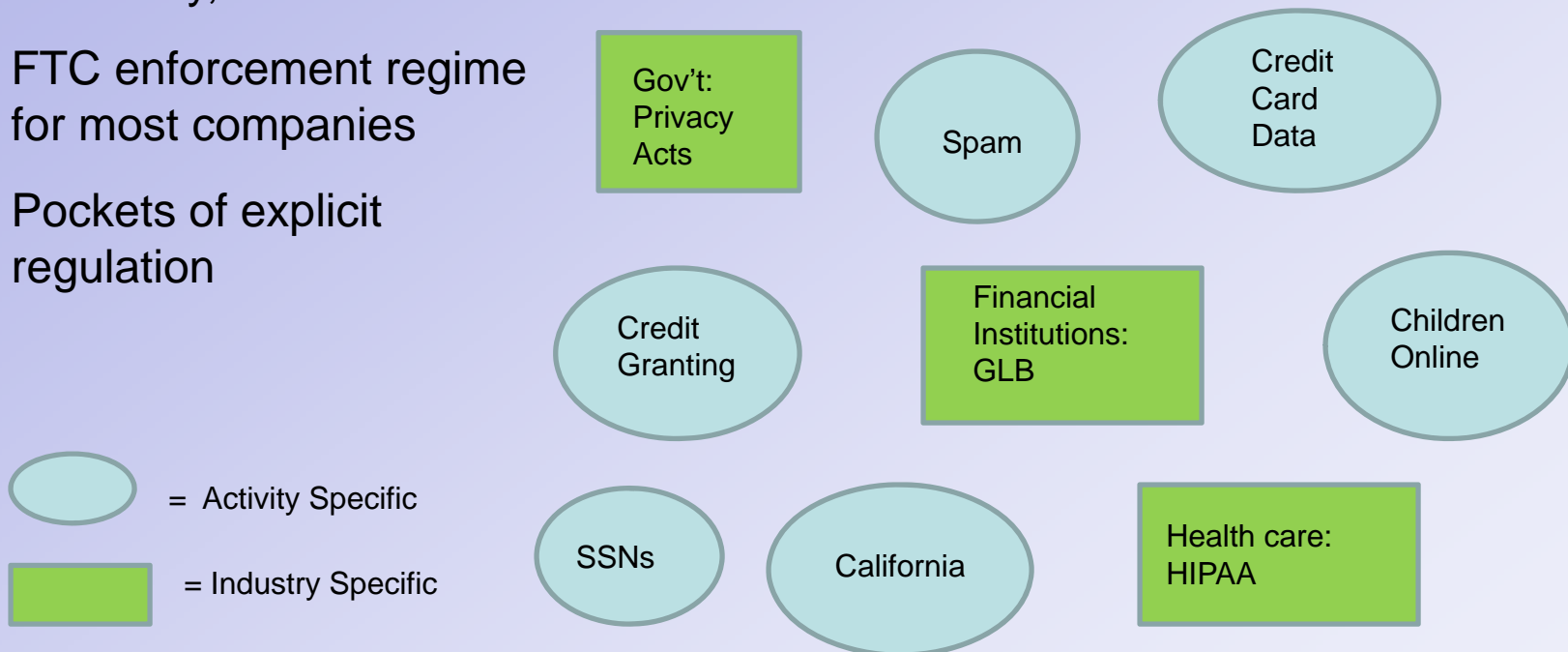
Tammy_Moskites@homedepot.com

The Current State of the Law



U.S. Regulatory Regime (For Now)

- Generally, market-based
- FTC enforcement regime for most companies
- Pockets of explicit regulation



FTC Sanctions

- Toysmart (2003) – tried to sell customer list as stand-alone asset in bankruptcy
- Education Research Center of America (2004) – said sharing data with educational institutions but actually sharing with marketing companies
- BJ's Wholesale (2005) – beginning a pattern of security cases continuing through today
- Sears (2010) – spyware loaded on computer with consent under long click-wrap agreement

Federal Trade Commission Regulation

- Authority under 15 U.S.C § 41-58 to curb “unfair and deceptive trade practices”
- Sanctions may be imposed at \$10,000 per violation
- Statute covers corporations organized for profit, but FTC takes position that regardless of charter, if substantial part of activities provide pecuniary benefit for members, then jurisdiction is proper (American Med. Ass’n., 1979).
- State statutes are similar in scope

Major Pockets of Regulation Affecting You

(Children's Online Privacy Protection Act)

CAN SPAM Act of 2003

(Telephone Consumer Protection Act)

California

Data breach laws

PCI/security standards enacted into law

SSNs



Children's Online Privacy Protection Act

- Does not apply to non-profits (15 U.S.C. § 1302(2))
- Applies to:
 - ✓ Operators of websites or online services directed at children under 13
 - ✓ Operators of general audience website with actual knowledge that you have information from children under 13
- Requires:
 - ✓ Notice on website with 8 specific areas of disclosure
 - ✓ Notice to parent with same information (can be e-mail, fax, regular mail)
 - ✓ "Verifiable consent" from parent before any information is collected
 - Faxed or mailed signature
 - Credit card with transaction
 - Parent calls 1-800 number

CAN SPAM Act of 2003

- Can apply to commercial messages by non-profits
- Criminal penalties for illegal harvesting of e-mails, accessing another's computer to send spam without permission, other "sneaky" practices
- E-mail formatting and processing provisions apply only to promotional e-mails
- Such e-mails must:
 - Use an accurate subject line
 - Identify sender and have an accurate header ("From")
 - Give mailing address
 - Provide an electronic means to opt out
- "Sender" must honor all opt-outs within 10 days of request

Telephone Consumer Protection Act (Do Not Call)

- Does not apply to tax-exempt non-profit organizations
- Federal law prohibiting marketing calls to any number registered on Do Not Call List
 - Exceptions for (1) “established business relationship,” meaning a purchase or two-way transaction within the 18 months before the call and (2) express written agreement allowing the calls
 - Safe harbor for callers that are using registry not more than 3 months old plus proper training and other procedures
- Calling/soliciting companies must also keep list of numbers who have requested not to be called again by that company
 - Unless circumstances would warrant, these requests do not apply to affiliates
- No calls before 8 am or after 9 pm

California: Strict Regime

Requirements:

- Online business having commercial website must post Privacy Policy of certain type size containing certain disclosures
- “Shine the Light” requires disclosures for “businesses” that share data for third party marketing purposes
- Often a trend-setter
 - ✓ First data breach law
- Usually enacts most strict standard among states
 - ✓ Opt-ins added to GLB for third party disclosures
 - ✓ “No harm required” standard in data breach law

State Breach Notice Laws

- 46 of the 50 states have breach laws now
- Protected information is generally first name/initial, last name in combination with any of: SSN, driver's license number, financial account number plus access code
 - Encrypted data is excepted out
- Require notice to affected individuals, sometimes also government agencies and credit bureaus
- Split among states whether there is a "risk of harm" threshold for notification
- A company need not do business in these states to be subject to these laws

Georgia Code: §10-1-911

Applies to “data collectors” and “information brokers”:

“Data collector” means any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity.

“Information broker” means any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties.

Definition of Personal Information: 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:

(a) Social security number; (b) Driver's license number or state Identification Card number; (c) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords; (d) Account passwords or personal identification numbers or other access codes; or (e) Any of the items contained in subparagraphs (a) through (d) above when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

Data Destruction Laws

- FACTA requires all businesses possessing “consumer information” for a business purpose to take reasonable measures to protect the information in the process of disposal
- State laws vary widely but are generally applicable to businesses
- OCGA §10-15-2 covers medical information, account information, tax return information and contents of applications for business accounts
 - Allows shredding, erasing and other methods reasonably believed to ensure no unauthorized access

PCI/Security Standards Enacted by States

- Payment Card Industry (PCI) standards are security standards for merchants and their service providers regarding transmission, processing and storage of credit card data
 - Unified standard set by outside council for whole payment card industry
- Effective in 2010, Nevada now requires compliance with PCI standards by law
- Massachusetts and Nevada both require encryption of personal information in transmission and on mobile devices such as laptops
 - Personal information encompasses SSN, drivers' license, financial account number plus access code

Social Security Numbers

- Patchwork of state laws
 - Almost all states limit public use of SSNs or use as password
 - Several states limit the sale of SSNs
 - Several states require special privacy policies if SSNs collected and used
- Moral of the story: eliminate use of SSNs or get specific advice

Service Provider under GLB/HIPAA

- May apply to provision of services or joint activities with banks/financial institutions or with health care companies/insurers
- Required agreements are not negotiable
- Best advice: restructure activity to avoid contact with these companies' data

Service Provider under GLB/HIPAA (Cont'd)

- The good: use data only for authorized purposes
- The bad: notify client if unauthorized disclosure or access, delete data on request of client
- The truly ugly: apply industry-standard security measures to protect the data
 - ✓ Encryption in storage and transit, penetration testing, vulnerability scans, strong passwords, written access logs...

The Commercial Privacy Bill of Rights Act of 2011

- On April 12, 2011 Senators John Kerry (D-MA) and John McCain (R-AZ) introduced legislation aimed at providing consumers with greater control over the collection and use of their personal information accessible through online and offline channels. ... would create baseline fair information practice protections for consumers similar to those outlined in the December 2010 Department of Commerce Privacy Green Paper. Such protections would include consumer notice prior to the collection of personal information, and opt-in or opt-out consent mechanisms depending on the type of personal information collected and its intended use.

The Commercial Privacy Bill of Rights Act of 2011

- If enacted, the bill would apply to "covered entities," which the bill defines as any person that collects, uses, transfers, or maintains personal information concerning more than 5,000 "individuals" within a single year. (The bill does not clarify whether the term "individuals" within this context applies to consumers, employees, or both.) – ***what about donors?***
- The bill specifically applies to non profits.

Key Components of a Privacy Program

- Privacy Policy
- Records Management Procedures
- Training, Communications, Enforcement, Monitoring

People – Process – Technology

The Privacy Policy

- Do you need one?
 - ✓ Yes, if you already have one available to the public
 - ✓ Yes, if your clients or other constituencies desire or require it
 - ✓ Yes, if you have a national commercial website

Otherwise:

NO, You Don't

The Privacy Policy

Key elements:

- Are you covered by any law dictating what you must disclose?
- Take a close look at your users and their expectations when they give you data
 - User surprise = key disclosure**
- Look at your capabilities as you make your undertakings
 - Overpromising = invitation to trouble**

Privacy Policy -- Best Practices

- Consider a mini-summary of key points
- Break out and disclose each of the following:
 - Types of data collected
 - Purpose of each collection
 - Sharing of data with third parties (don't forget M&A, bankruptcy!)
 - Choices for user
 - Security applied
 - How amendments work
 - Date of policy
- Interaction with T&C

Privacy Policy -- The No-No's

~~“Just this once ...”~~

~~Failure to follow own
Privacy Policy~~

~~Well, let's just change
it...”~~

~~Changing Privacy
Policy on the fly~~

**Remember: A Privacy Policy Unenforced is
Worse Than None At ALL!**

Records Management

- If your Privacy Policy is *WHAT* you do, your Records Management program is *HOW* you do it.
- Answers the question, “How do you protect my privacy and personal information?”
- Focus: The method by which an organization obtains, uses, distributes, stores and disposes of individuals’ private information.
- Objective: Know where the data is, protect it, and get rid of it when it no longer serves a legitimate business purpose.

Records Management Model



Questions and Discussion



For More Information:

If you would like more information about the services of Pro Bono Partnership of Atlanta, contact us at:

Phone: 404-407-5088

Fax: 404-853-8806

Info@pbpatl.org

www.pbpatl.org