710 Marketing Your Company's Services in an Opt-out World

Francis M. Caesar
Vice President–Legal Affairs
Barnesandnoble.com

Charles A.B. Moore
Associate Counsel
Federated Department Stores, Inc.

Althea Johnson Williams
Assistant General Counsel
LendingTree, Inc.

Faculty Biographies

Francis M. Caesar

Frank Caesar is vice president‹legal affairs at Barnesandnoble.com in New York. As head of Barnesandnoble.com's legal department, his responsibilities include negotiation of strategic marketing and technology agreements, legal review and support of all marketing programs, and management and oversight of outside counsel.

Prior to joining Barnesandnoble.com, Mr. Caesar served three years in the American Express general counsel's office, leaving as vice president-group counsel. He was the division attorney for American Express Relationship Services, the departments of which were responsible for American Express' internet initiatives, fee-based services, catalog marketing, student lending, and new product development. He also served as division attorney to the marketing department of Corporate Services, the division responsible for the American Express Corporate Card and Procurement Card. Mr. Caesar was an associate corporate attorney at the New York law firms of Thacher Proffitt & Wood and Breed, Abbott & Morgan.

He received his BA and JD from the University of Chicago.

Charles A.B. Moore

Charles A. B. Moore is associate counsel with Federated Department Stores. His responsibilities include electronic commerce, technology, commercial contracts, and regulatory matters.

Prior to joining Federated, Mr. Moore was transactional counsel for United Parcel Service in Atlanta and in private practice in Connecticut.

He is currently on ACCA's Board of Directors and cochairs ACCA's eCommerce Committee. Mr. Moore is immediate past president of ACCA's Georgia Chapter. He is a member of the Computer Law Association and is a frequent speaker on technology and eCommerce issues. He is a member of the Board of Directors for the Carrie Steele-Pitts Home in Atlanta, which provides a secure home for neglected and abused children.

Mr. Moore is a graduate of Trinity College and received his JD from Vermont Law School.

Althea Johnson Williams
Assistant General Counsel
LendingTree, Inc.

STATE STATUTES REGARDING UNSOLICITED COMMERCIAL E-MAIL

1. **Arkansas**

   Unlawful Acts Involving Electronic Mail.
   - Ark. Stat. Ann. §5-41-205.

2. **California**

   Faxing or E-Mailing of Unsolicited Advertising Materials; Toll- Free Telephone Number.
   - Cal. Business & Professional Code §17538.4.

   Electronic Mail Service Providers; Policy For Initiation of Unsolicited Electronic Mail Advertisement by Registered User; Actions For Violations.
   - Cal. Business & Professional Code §17538.45.

3. **Colorado**

   Colorado Junk Email Law.
   - Colo. Rev. Stat. §6-2.5-101 et seq.

4. **Connecticut**

   Computer Crimes.
   - Conn. Gen. Stat. §53 - 453.

5. **Delaware**

   Computer Related Offenses.
   - Del. Code Ann. tit.11 §931 et.seq.

   Unrequested or Unauthorized Electronic Mail or Use of Network or Software to Cause
   - Del. Code Ann. tit.11 §937.

6. **Idaho**

   Unfair Bulk Electronic Mail Advertisement Practices.
   - Idaho Code §48-603E.

7. **Illinois**

   Electronic Mail Act.
   Unsolicited or Misleading Electronic Mail; Prohibition.
   - 815 Ill. Comp. Stat. Ann. §511/10.

8. **Iowa**

   Electronic Mail Transmissions.
   - Iowa Code Ann. §714E.1 & 714E.2.

9. **Kansas**

Commercial Electronic Mail Act.
- Senate Bill 467 (Enacted May 17, 2002).

10. **Louisiana**

Computer Related Crimes.
Offenses Against Electronic Mail Service Provider.
- La. Rev. Stat. Ann. §14:73.6.

11. **Maryland**

Electronic Mail - Unauthorized, False, or Misleading Information.
- Senate Bill 538 (Enacted May 6, 2002; effective October 2002).

12. **Minnesota**

Commercial Electronic Mail Solicitation.
- Senate File No. 2908 (Enacted May 20, 2002; effective March 1, 2003).

13. **Missouri**

Electronic Mail Practices
- Mo. Rev. Stat. §407.1120 et seq.

14. **Nevada**

Unlawful Acts Regarding Computers And Information Services
- Nev. Rev. Stat. Ann. §205.473 et seq.
  See Nev. Rev. Stat. Ann. §205.492--Unlawful Acts Involving Electronic Mail or Transmission of other Data, Information, Images, Programs, Signals or Sounds to Computer, System or Network.

15. **North Carolina**

Computer-Related Crime.
- N.C. Gen. Stat. §14-453 et seq.

16. **Ohio**

Internet Privacy
- Senate Bill No. 8 (Enacted August 2002; effective November 1, 2002).

17. **Oklahoma**

Fraudulent Electronic Mail.
- Okla. Stat. tit.15, §776.1 et seq.

18. **Pennsylvania**

Dissemination of Explicit Sexual Material Via an Electronic Communication.
- 18 PA. Cons. Stat. § 5903(a.1).

19. **Rhode Island**

Computer Crime.
- R.I. Gen. Laws §11-52-1.

Unsolicited Electronic Mail.
- R.I. Gen. Laws §6-47-2

20. **South Dakota**

Deceptive Acts or Practices.
- S.D. Codified Laws Ann. §37-24-6(13).

Transmission of False or Misleading Electronic Mail Messages Prohibited.
- S.D. Codified Laws Ann. §37-24-37.

21. **Tennessee**

Unsolicited Faxed or E-Mailed Advertising, Regulation; Damages.
- Tenn. Code Ann. §§ 47-18-2501-2502.

22. **Utah**

Unsolicited Commercial or Sexually Explicit E-Mail—Requirements.
- Utah Code Ann. §13-36-103.

23. **Virginia**

Virginia Computer Crimes Act.
- VA. Code Ann. §18.2-152.1et seq.

24. **Washington**

Commercial Electronic Mail
- Wash. Rev. Code Ann. §19-190 et seq.

25. **West Virginia**

Electronic Mail Protection Act.
- W. VA. Code §46A-6G-1 et seq.

26. **Wisconsin**

Sending Obscene or Sexually Explicit Electronic Messages.
- Wis. Stat. Ann. §944.25

Marketing in an Opt-Out World- Privacy Policies

ACCA

October 22, 2002

Frank Caesar
Vice President – Legal Affairs
Barnesandnoble.com

Opt-out vs. Opt-in

- In the context of marketing:
  - opting-out requires affirmative steps by an individual to prevent the collection, use or transfer of personally identifiable information;
  - opting-in requires affirmative steps by the individual to allow such collection, use or transfer of PII

Personally identifiable Info

Individually identifiable information from or about an individual including (but not limited to):

- –Name
- –Home address
- –E-mail address or other online contact information
- –Telephone number
- –SSN
- –A persistent Identifier (e.g., cookie, computer serial code)

Privacy Policy

- A privacy policy is a business' statement of its collection, use and sharing policies with respect to personally identifiable marketing information
- At a minimum, a privacy policy is a representation by a company made to induce a user of a site or service to provide information (personally identifiable or not)

Privacy –Policy – cont'd

Generally there are no legal requirements to post a privacy policy. However, when a policy is posted, failure to adhere to its terms could be construed as an "unfair and deceptive" trade practice

- There are industry segment exceptions

Sound Business Practice

Why Have a Privacy Policy if Not Legally Required?:

- A business practice that consumers are becoming increasingly savvy to look for
- It helps potential customers get over their fears of using the Internet
- Your competitors have it.

Sound Practice – cont'd

- A well written privacy policy can shied a company from future liability and promote user confidence and goodwill
- A poorly, "overly complex," or ambiguously written policy can cause difficulty for the company

Sound Practice – cont'd

Failure to adhere to stated privacy policy will result in an "unfair and deceptive" characterization of an entity's business practice, hence subject such practice to actions by the FTC, state attorneys general and others (private litigants).

Privacy Policy Contents – Fair Information Practice Principles

A concise set of guiding principles are the Fair Information Practice Principles (FIPP) identified by the FTC.

FIPP – cont'd

(1) Notice/Awareness
(2) Choice/Consent
(3) Access/Participation
(4) Integrity/Security
(5) Enforcement/Redress

FIPP - cont'd

Notice/Awareness:

- Consumers should be given notice of an entity's information practices before any personal information is collected from them.

FIPP - cont'd

Choice/Consent:

- Choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information -- *i.e.*, uses beyond those necessary to complete the contemplated transaction.

FIPP - cont'd

Access/Participation:

- This refers to an individual's ability both to access personal data about him or herself -- *i.e.*, to view the personal data in an entity's files -- and to contest that data's accuracy and completeness.

FIPP - cont'd

Integrity/Security. Data should be accurate and secure.

- To assure data integrity, collectors must take reasonable steps, such as using only reliable sources of data.
- Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.

FIPP - cont'd

Enforcement/Redress.

- The core principles of privacy protection can only be effective if there is a mechanism in place to enforce them.

What not to put in a privacy policy

- Material obligations on the part of the user (other than instructions)– a policy is typically not affirmatively accepted
- Unrealistic guarantees
- Make a change to your policy that has a material and adverse retroactive effect

Overview of the Privacy Provisions of the Gramm-Leach-Bliley Act.

- The purpose of the Gramm-Leach-Bliley Act (GLB) is to protect consumer information collected and retained by Financial Institutions.

- GLB restricts the ability of Financial Institutions to disclose nonpublic personal information (NPI) about consumers to nonaffiliated third parties.
- Also restricts use of NPI received from Financial Institutions by entities not covered by GLB.
- GLB does not restrict sharing NPI with affiliates of Financial Institutions.

- **Definitions**
  - Financial Institutions
  - Nonpublic Personal Information (NPI)
  - Consumer
  - Customer

Financial Institution

- Includes not only traditional depository institutions, but also institutions whose activities have been determined to be financial in nature and those that are incidental to the banking industry.
- Business must also be significantly engaged in such financial activities

Nonpublic Personal Information (NPI)

- Includes all information that is not publicly available that a financial institution obtains from a consumer in connection with providing a financial product or service.

Consumer

- An individual that obtains or has obtained a financial product or service from a Financial Institution to be utilized primarily for personal or household purposes.
- GLB does not apply to commercial clients.

Customer

- Typically has a significant and on-going relationship with the Financial Institution.

- **GLB imposes three general privacy obligations upon Financial Institutions**:
  - Notice
  - Opportunity to “opt out”
  - Protect NPI

Opportunity to "opt out"

- Financial Institutions must provide consumers and customers with an opportunity to opt-out before sharing NPI with non-affiliated third parties.

Protect NPI

- Financial Institutions must institute data security and other mechanisms to protect NPI collected and retained by the Financial Institution *(will not be covered in this presentation).*

Notice

- Financial Institutions must provide notice to consumers and customers of its NPI handling practices.

Consumers

- Consumers are only entitled to receive a privacy notice if the Financial Institution shares NPI with third party non-affiliates.

Customers

- Financial Institutions must provide notice to its **customers** of its NPI handling practices even if the entity does not share NPI with non-affiliated third parties.
- Privacy notice must be provided at least every twelve months.

Privacy Notice

- Must outline the privacy practices of the Financial Institution.
- Written notice must be provided at the time the consumer relationship is established. Notice can be provided via mail, electronically or in person.
- If Financial Institution shares NPI with third party non-affiliates, notice must also provide consumers and customers with a reasonable instructions to opt-out and reasonable period of time to opt out.

Privacy Notice

- Must include certain specific information. Primary information that must be included:
  - Categories of information that the Financial Institution collects;
  - Categories of information disclosed by the Financial Institution;
  - Categories of affiliates and non-affiliates to whom the Financial Institution discloses NPI;
  - Policies and practices for protecting the NPI collected by the Financial Institution.

Opt-out Directives

- Financial Institution can determine the steps required to opt out; however, steps must be reasonable.
- Valid after the termination of the customer relationship.
- Must be complied with by Financial Institution as soon as reasonably possible.

State Preemption

- GLB does not preempt state law; thus individual jurisdictions are free to pass laws that provide greater protection than GLB. Most states use an opt-in provision.
- States with some form of opt-in provisions AK,CT, IL, MD, ND & VT.
- After opt-in legislation in CA failed, San Mateo County and Daly County adopted opt-in ordinances.

GLB does not allow consumers to opt-out of all information sharing by a Financial Institution.

- Allows Financial Institutions to share NPI with affiliates;
- General Exceptions Sec. 503 (e)

