Session 309

Preventive Law for Small Law Departments and Generalists

Lael Bellamy
Senior Attorney
ChoicePoint Inc.

Jonathan J. Soll
Senior Counsel - Information Technology
Georgia-Pacific Corporation

Darity Wesley
Corporate Counsel
Acxiom-Dataquick Products Group

ChoicePoint

The Fair Credit Reporting Act: Its Scope is Broader Than You May Realize

Lael Bellamy

Senior Attorney

1999 ACCA Annual Meeting

November 4, 1999

Topics

- FCRA History
- How Might the FCRA Impact Your Business?
- Definitions
  - What is a Consumer Report?
  - What is an Investigative Consumer Report?
  - Permissible Purpose
  - What is an Adverse Action?
- Conditions for Furnishing Reports
  - Certification from Recipients
  - Conditions for Furnishing Employment Reports - Certification from Recipients

Topics

- Requirements for Recipients
  - Consumer Reports - Adverse Action
  - Employment Reports - Pre-authorization
  - Employment Reports - Adverse Action
  - Investigative Consumer Reports - Disclosures
  - Consumer-Type Reports from Third Parties - Adverse Action
  - Consumer-Type Reports from Affiliates - Adverse Action
  - Consumer Reports Containing Medical Information
- Limits on Information in Reports
- Liability For Violations Of The FCRA
- Resources for Additional Information

FCRA History

- Cite: 15 U.S.C. section 1681, et seq.
- Originally passed in early 1970's
- Designed to protect consumers from inaccurate information in consumer reports and to limit the use of consumer reports to certain purposes
- Significant Amendments
  - Passed in September 1996
  - Effective as of October 1997
- Latest Amendments
  - Passed in November of 1998
  - Effective as of November 1998

How Might the FCRA Impact Your Business?

- FCRA amendments regarding employment reports affect both the employer and the employee and failure to follow the rules may expose company to liability
- Improper use of FCRA and non-FCRA reports ordered for due diligence may expose company to liability
- Improper use of FCRA and non-FCRA reports ordered for insurance purposes may expose company to liability
- Reports from affiliated companies and other third parties may be governed by the FCRA

How Might the FCRA Impact Your Business?

- Additional sections of the Act apply if you use consumer reports for granting credit, underwriting insurance, prescreening for credit or insurance, screening tenants, determining eligibility for government benefits, or valuing or assessing the risks of an existing credit obligation or if you contribute information to a consumer reporting agency
  - Because these provisions are specific to particular businesses, they will not be covered in this presentation

What is a Consumer Report?

- Generally, a Consumer Report is any written, oral, or other communication of any written information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for --

  (A) credit or insurance to be used primarily for personal, family, or household purposes;

  (B) employment purposes; or

  (C) certain other purposes authorized under the FCRA.

What is a Consumer Report?

- The definition includes:
  - public records, including criminal records and motor vehicle records, ordered from a third party for employment or personal insurance purposes;
  - background checks performed for employment purposes by a third party, including work by private investigators; and
  - credit reports ordered from a third party that sells them for credit, employment or personal insurance purposes.

What is an Investigative Consumer Report?

- Generally, an Investigative Consumer Report is a special type of consumer report in which information on a consumer's character, general reputation, personal characteristic, or mode of living is obtained through personal interviews with individuals who may have knowledge concerning any such items of information.

What is an Investigative Consumer Report?

- The definition includes:
  - Reference checks ordered from a third party company for employment purposes.

Permissible Purpose

- You must have a permissible purpose to order a consumer report. Permissible purposes include:
  - evaluating a consumer for employment, promotion, reassignment or retention as an employee;
  - underwriting of insurance involving the consumer;
  - a credit transaction involving the subject of the report and involving the extension of credit to, or review or collection of an account of the consumer; and
  - the written authorization of the subject of the report.

What is an Adverse Action?

- Adverse Actions include all business, credit, and employment actions affecting consumers that can be considered to have a negative impact -- such as unfavorably changing credit or contract terms or conditions, denying or canceling credit or insurance, offering credit on less favorable terms than requested, or denying employment or promotion.

Conditions for Furnishing Reports - Certification from Recipients

- To receive consumer reports, you must
  - certify the purposes for which the information is sought; and
  - certify that the information will be used for no other purpose.

Conditions for Furnishing Reports - Certification from Recipients

- Potential risk areas:
  - if you get a report for due diligence purposes based on the written authorization of the consumer, you cannot take adverse employment action based on that report.
  - if your insurer gets reports on individuals to underwrite your corporate insurance, you cannot take adverse employment action against the individual based on that report.

Conditions for Furnishing Employment Reports - Certification from Recipients

- You can receive consumer reports for employment only if you certify:
  - your purpose for requesting the report (employment purposes) and that the information in the report will be used for no other purpose;
  - that before a consumer report is procured, you will comply with the disclosure and pre-authorization requirements;
  - if you are ordering an investigative consumer report, that you have complied and will comply with the additional disclosure requirements for those reports;
  - that before you take any adverse action on the report, you will give the consumer a copy of the report and the consumer statement of rights; and
  - that the information from the report will not be used in violation of federal or state equal opportunity law.

Requirements for Recipients of Consumer Reports

- If you have a permissible purpose, other than an employment purpose, for ordering a report, you do not have to give pre-notification to or get pre-authorization from the consumer except when required by state law (see NY and VT FCRA laws).
- For employment consumer reports, there are specific pre-authorization and pre-adverse action requirements.
- For investigative consumer reports, there are special disclosure requirements.
- Whenever you take adverse action based on a consumer report or a consumer-type report, you have certain responsibilities.

Requirements for Recipients of Consumer Reports - Adverse Action

- At the time of the adverse action, you must provide the consumer with oral, written or electronic notice of
  - the adverse action;
  - the name, address and toll-free telephone number of the consumer reporting agency;
  - a statement that the consumer reporting agency did not make the decision to take the adverse action and is unable to provide the consumer the specific reasons why the adverse action was taken;
  - the consumer's right to obtain a free copy of a consumer report from the consumer reporting agency for 60 days; and
  - the consumer's right to dispute the accuracy or completeness of any information in a consumer report furnished by the consumer reporting agency.

Requirements for Recipients of Employment Reports - Pre-authorization

- You must provide written disclosure to the consumer in a stand alone document that a consumer report may be obtained for employment purposes; and
- You must get written authorization from the consumer to procure the report, before ordering the report

Requirements for Recipients of Employment Reports - Adverse Action

- **Before** you take any adverse action on a employment report, you must give the consumer a copy of the report and the consumer statement of rights.

Requirements for Recipients of Investigative Consumer Reports - Disclosures

- You must follow all requirements for consumer reports
- In addition, you must disclose to the consumer in writing mailed or delivered not later than 3 days after the report is requested
  - that an investigative consumer report, including information as to character, general reputation, personal characteristics and mode of living, whichever applicable, may be made;
  - a statement informing the consumer of the right to additional disclosures under FCRA; and
  - the summary of consumer rights.

Requirements for Recipients of Investigative Consumer Reports - Disclosures

- If, within a reasonable time after receiving initial disclosure, the consumer requests additional disclosures, you must make a complete and accurate disclosure of the nature and scope of the investigation requested.
- Disclosure must be mailed or delivered by the later of 5 days after
  - you receive the request from the consumer; or
  - the date the report was requested.

Requirements for Recipients of Consumer-Type Reports from Third Parties- Adverse Action

- If you deny (or increase the charge for) credit or insurance for personal, family, or household purposes based either wholly or partly upon information from an entity other than a Consumer Reporting Agency, and the information is the type of consumer information covered by the FCRA,
  - you must clearly and accurately disclose to the consumer his or her right to obtain disclosure of the nature of the information that was relied upon by making a written request within 60 days of notification; and
  - you must provide the disclosure within a reasonable period of time following the consumer's written request.

Requirements for Recipients of Consumer-Type Reports from Affiliates - Adverse Action

- If you take adverse action involving insurance, employment or a credit transaction initiated by the consumer, based on information of the type covered by the FCRA, and this information was obtained from an entity affiliated with your company by common ownership or control, you must notify the consumer of the adverse action.

Requirements for Recipients of Consumer-Type Reports from Affiliates - Adverse Action

- The notification must inform the consumer that he or she may obtain a disclosure of the nature of the information relied upon by making a written request within 60 days of receiving the adverse action notice.
- If the consumer makes such a request, you must disclose the nature of the information not later than 30 days after receiving the request.

Requirements for Recipients of Consumer-Type Reports from Affiliates - Adverse Action

- Information that is obtained directly from an affiliated entity relating solely to its transactions or experiences with the consumer, and information from a consumer report obtained from an affiliate are not subject to these requirements.

Requirements for Recipients of Consumer Reports Containing Medical Information

- Consumer reporting agencies cannot provide consumer reports that contain medical information for employment purposes, or in connection with credit or insurance transactions, without the specific prior consent of the consumer who is the subject of the report.
- In the case of medical information being sought for employment purposes, the consumer must explicitly consent to the release of the medical information in addition to authorizing the obtaining of a consumer report generally.

Limits on Information in Reports

- Consumer reporting agencies cannot report any adverse information that antedates the report by more than 7 years, except that:
  - bankruptcies may be reported for 10 years after date of entry of the order for relief or date of adjudication;
  - records of convictions of crimes may be reported (new in the 1998 amendments);
  - civil suits, civil judgments and records of arrests may be reported for the later of
    - 7 years; or
    - until the governing statute of limitations expires.

Limits on Information in Reports

- Limitations do not apply to consumer credit reports used in connection with:
  - a credit transaction involving, or which may reasonably be expected to involve, a principal amount of $150,000 or more;
  - the underwriting of life insurance involving, or which may reasonably be expected to involve, a face amount of $150,000 or more; or
  - the employment of any individual involving at any annual salary which equals, or which may reasonably be expected to equal $75,000, or more.

Liability For Violations Of The FCRA

- Failure to comply with the FCRA can result in state or federal enforcement actions, as well as private lawsuits.
- Any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution.

Resources for Additional Information

- FTC Web Site: www.ftc.gov
  - Text of the FCRA: www.ftc.gov/os/statutes/fcra.htm
  - Index of Staff Opinion Letters on FCRA Issues: www.ftc.gov/os/statutes/fcra/index.htm
  - Site also contains Consumer's Statement of Rights Under the FCRA, Obligations of Users and Obligations of Furnishers
    - These statements were drafted by the FTC, as required by the 1997 FCRA amendments, and are distributed to consumers, users and furnishers by consumer reporting agencies.

Resources for Additional Information

- Associated Credit Bureaus
  1090 Vermont Avenue, NW
  Suite 200
  Washington, D.C. 20005-4905
  202/371-0910
  - Trade association of credit bureaus
  - Publishes an inexpensive, but very thorough, clause by clause interpretation of the FCRA entitled, How to Comply with the 1997 Fair Credit Reporting Act

Resources for Additional Information

- FTC's Commentary on the FCRA: 16 CFR Part 600 Appendix
  - Please note that this commentary has not been updated since the 1996 amendments to the FCRA.

MANAGING ELECTRONIC DATA RISKS THROUGH AN E-MAIL RETENTION POLICY

Jonathan J. Soll, Esquire
Georgia-Pacific Corporation
Atlanta, Georgia

TABLE OF CONTENTS

I. Introduction

The subject of a company creating and implementing an e-mail policy is no longer back page news. It should be a mantra among information technology attorneys that to be effective, an e-mail policy must at least state 1. that the e-mail systems are owned by the company and are solely for business use; 2. that e-mail messages and mail boxes are not private and can be monitored or accessed by the company notwithstanding any use of passwords; 3. the types of e-mails that are prohibited[1]; and 4. that policy violators are subject to disciplinary action, up to and including termination. An e-mail policy containing the above concepts is relatively easy to write and implement once you overcome the expected new policy challenges of convincing management of its necessity, and determining how strictly the policy will be enforced.[2]

While there has been much written on the importance of having and implementing an e-mail policy, there has not been as much written about having an e-mail retention policy as a means to manage risk. A properly implemented e-mail retention policy, in combination with a well drafted e-mail policy, can help reduce the risk of e-mail messages leading to liability. As a collateral benefit, the process of designing and implementing an e-mail retention policy (see Section IV below) has the potential to reduce e-mail discovery compliance costs through increased efficiencies, because you will gain a better understanding of how your company's e-mail systems can collect, sort and store e-mail. E-mail retention may not be as glamorous to discuss as the issues surrounding drafting and implementing an e-mail policy, such as employers' e-mail monitoring rights versus employees' privacy rights, but it has at least the same potential to reduce liability.

While many companies already have a policy governing the retention of paper documents, such policy is unlikely to address the issues specific to electronic messages. For example, a paper document retention policy probably contains a retention period that is too long for electronic

messages[3], and is unlikely to address automated enforcement [4] and e-mail discovery compliance[5], which are only relevant in the electronic realm. The practices of using e-mail to send potentially offensive material (e.g. jokes and pictures) and being dangerously casual with the content of business discussions over e-mail are pervasive among e-mail users. These practices, coupled with the fact that many e-mail users are unaware that deleted e-mail messages may be recoverable and are likely to be discoverable, warrant a special policy to govern e-mail retention. The risks inherent with e-mail are compounded because messages are often sent to multiple parties (what I like to call the "cc" devil), resulting in long-chained e-mails. Having an effective e-mail use and retention policy helps address these risks.[6]

Before proposing an action plan to implement an e-mail retention policy, it is beneficial to discuss the core substantive issues involved, such as the discoverability of e-mails, realistic scope of the problem, and why the risks of e-mail leading to liability are real.

II. The Discoverability of E-mail Messages

Electronically stored data (which includes e-mails) is generally discoverable in a lawsuit. In Federal courts for example, Federal Rule of Civil Procedure (F.R.C.P.) 34(a), which permits discovery of documents and usable data compilations, has been defined by courts to include electronic documents and specifically, e-mails. Compliance with e-mail discovery is mandatory and can be extremely costly, even when no damaging content is discovered.

For example, in an antitrust litigation brought against CIBA-Geigy Corporation ("CIBA"), a discovery demand under F.R.C.P. 34(a) was issued requiring disclosure of various categories of e-mails stored on CIBA's back-up tapes which were calculated by CIBA to amount to nearly 30,000,000. CIBA argued to the court that it would cost them between $50,000 and $70,000 to search and reformat such e-mails and that the plaintiff should bear the costs. After holding that

e-mails are discoverable under F.R.C.P. 34, the court rejected CIBA's argument and ordered CIBA to produce the e-mails. The court held that the normal and reasonable translation of electronic data into a usable form is a foreseeable and necessary burden of litigation and, in the absence of showing of undue hardship, CIBA (and all other similar defendants) would have to bear their own costs.[7]

It is well settled law that any party in a lawsuit must produce e-mails in discovery. Lawsuits are often settled because the cost of discovery and litigation is forecast to be higher than the cost to settle. While undue hardship may be argued, the CIBA court's holding makes such argument difficult to sustain if based only on the cost to produce the e-mails. It is arguable, therefore, that it will soon be standard operating procedure to use e-mail discovery to drive up the risk and litigation costs to extract large settlements. Companies with long e-mail retention periods, or no policy at all, will be particularly good targets for this new "smart-weapon."

III. Typical Scope of the Problem

In order to understand the level of risk of long term e-mail retention, it is helpful to discuss a hypothetical company. The E-mails Forever Company has 10,000 employees, who all use the Company's e-mail system. Between sending and receiving e-mails, the average user at E-mails Forever stores 20 new e-mails on his or her computer per day.[8] Therefore, approximately 200,000 new e-mails per day are stored on E-mails Forever's e-mail computers (commonly called e-mail servers). There is no formal policy at E-mails Forever concerning retention of e-mails, and the only thing preventing them from storing e-mail messages forever is disk space. While they don't have unlimited capacity, E-mails Forever can save an entire year's worth of e-mails, without running out of disk space. At the rate of 200,000 per day, and approximately 22 business days per month, that adds up to 4,400,000 e-mail messages per month and 52,800,000 per year.[9] Even assuming that only 10% of such e-mails are actually saved, the

number would still be an astounding 440,000 e-mails per month. The actual number might be even twice as high or greater because many e-mails are sent to more than one user at the same time, as discussed above.

As this article will illustrate, all it takes is one inappropriate e-mail to cause substantial liability. If served with a discovery demand seeking e-mails, E-mails Forever is at substantial risk. At the very least, it would cost E-mails Forever a substantial amount of money just to sift through all of the e-mails they have saved. The cost in time and money might be high enough to cause them to settle the case, even if they believe they might ultimately prevail. Additionally, with such a large number of e-mails saved, they are likely to find at least some e-mails that assist their adversary's case. E-mails Forever would have benefited from an e-mail retention policy.

IV. Examples of Recent E-mail Cases that Led to Liability

There are several categories of causes of action brought against companies using the company's own e-mails as evidence. Among them are sexual harassment, racial discrimination, and one of the most potentially damaging, antitrust. E-mails can be a treasure-trove of information and admissions for lawyers to use in a lawsuit. Here is a brief example of each:

A. Sexual Harassment.

At Chevron Corporation, e-mails containing derogatory jokes about women such as, "25 reasons why beer is better than women," was a factor that led to a $2.2M out-of-court settlement of a sexual harassment lawsuit filed by 4 female employees.[10]

Using e-mail to send potentially offensive jokes is commonplace and people who send or save such jokes often do not realize that they are not written in disappearing ink and are both offensive and subject to discovery in a lawsuit. While a company can prohibit the

use of its e-mail systems to send jokes and can raise awareness of the risks, changing the casual way that people treat e-mails will not be easy and will likely require training and a cultural change in the way e-mail is used.

B. Racial Discrimination.

In Rodney King's civil lawsuit, the court allowed the admission of e-mails that were sent between police squad cars the night Mr. King was beaten by police as evidence of racial bias toward proving motive. In one such e-mail, a police officer commented, "Sounds almost (as) exciting as our last call … It was right out of 'Gorillas In the Mist.' " As we know, the Rodney King case was settled for approximately $1,000,000.[11]

Similarly, in Owens and Hutton v. Morgan Stanley, two African-American employees sued their investment banking firm employer and the employees who allegedly sent racist e-mail jokes directed at them over the company's e-mail system.[12] As is common with these types of lawsuits, the complaint sought relief under Federal law by claiming that the racist e-mail created a hostile work environment and discrimination under Title VII.[13] In addition to being offensive, racist jokes create unnecessary legal risk. The lawsuit, in which each plaintiff sought $30 million dollars in damages,[14] was settled on February 10, 1998 for an undisclosed amount.[15]

C. Antitrust.

The Microsoft case has received widespread publicity in recent months. However, many people do not realize that e-mails that had been retained for relatively long periods of time are being used by the Justice Department as key evidence against Microsoft. The anti-trust experts have commented that the contents of such e-mails constitute some of the most damaging evidence against Microsoft.

Among them is an e-mail purportedly authored by Bill Gates in which he discusses his efforts to persuade Intuit's CEO not to distribute Netscape's Internet Browser with Intuit's financial software. The e-mail states, "I was quite frank with him that if he had a favor we could do for him that would cost us something like $1M to do that in return for switching browsers in the next few months, I would be open to doing that."[16]

These are but a few examples of how e-mails retained for relatively long periods of time can lead to costly discovery and large out-of-court settlements. In addition to the hard dollar costs, such lawsuits often come with headlines of bad publicity, which can result in various adverse business consequences, such as a decrease in a company's stock price.

V. Arguments Made by E-mail Users Against Record Retention

Common arguments made by e-mail users for not wanting to follow or being out of compliance with an e-mail retention period usually range from, "It is too inconvenient to go back through my e-mails on a regular basis and figure out what to erase" to "I have important business documents that I need for longer than the retention period and we should be able to treat electronic messages and attachments the same way we treat and retain paper documents today."

Employees having an equivalent-to-paper electronic filing cabinet[17] may be in our future. Some companies may already have such system. However, until the widespread custom of treating e-mails far more casually than hard-copy documents begins to change, printing out and saving legitimate business messages while deleting the rest is the only way to effectively reduce the risks associated with e-mail discovery. Of course, even this will only reduce the risks if a "print and delete" policy actually causes users to review e-mails before they decide whether or not to

print, rather than just printing everything without review. It is arguable that employees are likely to be more cautious about what printed documents they save, and therefore, a "print and delete" strategy has validity.

On the other hand, e-mail attachments in contrast to the body of an e-mail message, may warrant special treatment. Depending on how your company uses its e-mail systems, there may be validity in allowing long term retention of e-mail attachments such as final versions of word processing, spreadsheet documents and the like. An equivalent-to-paper electronic filing cabinet might work for legitimate business attachments, especially if your company can create rules and standards for storing such electronic documents[18] However, if users type such documents into the body of the e-mail message, along with an e-mail message about the document, long term storage will be more problematic.

VI. Action Plan to Implement E-Mail Retention Policy

Here are some steps to consider that may lead to an acceptable and implementable e-mail retention policy. As you will see, such steps can also be used to help create or improve an underlying e-mail policy:

1. Create New or Review and Update Existing E-Mail Policy.

There are many synergies to be gained between creating, implementing and enforcing an e-mail policy and an e-mail retention policy.[19] Therefore, if your company does not have an e-mail policy, one should be created and employees should be educated on its existence and content. Following the steps in this action plan is bound to help with that effort. If your company already has an e-mail policy, review it and make sure you are satisfied with its content. Once you are satisfied, determine the level of compliance, monitoring and enforcement you will seek, and use the remaining steps in

this action plan to come up with meaningful recommendations for improvements. If you did not write the policy and the person or group that did is still employed by your company, discuss the background with them and review their applicable files. That can help you save time with other steps in the action plan.

Before you get too far into the action plan, it would also be helpful to determine if your company has a paper record retention policy. If it does, read and understand it. Think about its content as you follow these steps to ensure that the e-mail and paper retention policies are consistent and read well together. Also, if your company decides to allow long term electronic retention of certain types of electronic documents (as discussed in Section V., above), then, for consistent-to-paper treatment, such electronically stored documents should be made subject to the paper document retention policy. Therefore, you should read such policy to make sure it would apply properly and determine whether any changes are necessary.

2. Understand Your Corporate Culture's Use of E-Mail.

Talk to employees at all levels of your company and try to understand how e-mail is used in your specific business. Does your company use e-mail only as a tool to set up meetings and lunch appointments, or do they type documents in the body of e-mail messages and use e-mail to engage in substantive business discussions? Does the average user at your company send e-mails populated with content that is more causal than the content of written memos? How prevalent is the use of e-mail for non-business purposes, such as to send jokes and to take part in personal discussions? Answering these questions will help you determine what level of risks exists and how long of a record retention period is desirable.

3. How Does Your Company Manage E-Mail Space?

To better gauge the challenges of affecting a cultural change in the use of e-mail, it would be helpful to first determine how the average e-mail user manages his or her disk space[20]. Ask yourself the following questions:

(i) How much disk space is made available to each user and how many days worth of e-mail fits in that space with the average user?

Your company's e-mail administrator(s) should be able to assist with obtaining this information, which will help you determine the volume of e-mail that you will potentially have to sort through in discovery. When the volume at your company is coupled with the content of the average e-mail, you will be better able to determine the level of risk.

(ii) Do your e-mail administrators routinely make more disk space available upon request?

If they do, the volume of e-mails saved has the potential to be large.

(iii) Does the average e-mail user have a legitimate review and filing method for managing their own e-mail folders? For instance, do they keep e-mail until they run out of space and then decide what to do, or do they delete e-mails as they are read, printing and saving only those of importance?

(iv) After a user runs out of disk space, do they just move the e-mails somewhere else on the system (e.g. a floppy disk or local hard drive), or do

they go through a legitimate review process?

If users are simply moving old messages to a floppy disk or local hard drive, the risk will obviously be greater, and you will be faced with the additional challenge that any automated monitoring and compliance methods that you use will likely not work outside of the e-mail servers (see paragraph 6, below).

(v) Does your company want to implement an electronic filing cabinet or a print and delete strategy?

As stated previously, having an electronic filing cabinet that is the electronic equivalent of its paper cousin may be in our future. However, before you jump into it, understand that in order for it to be a true equivalent from a content risk perspective, the average user would have to exercise the same level of scrutiny that they use for memos and other paper documents. That means that casual content would have to be significantly stemmed, which is the single largest challenge. Much more training and monitoring of employees would be required to equalize the risks of electronic message storage with those normally found with paper documents. While there are also risks with paper documents, I would argue that most employees are still far more casual with what they say in e-mails.

A print and delete strategy, on the other hand, is much easier to train on and implement. E-mail users would still have to be educated and trained to be less casual when writing e-mails. However, with a print and delete as you go policy, e-mail messages to be retained must be printed and stored as if it were a hard

copy documents. If an e-mail message is too casual, or not business related, it should be deleted after being read and not be printed. Even if the user does not choose what to print and delete every day, they will have to do so by the end of the e-mail retention period or the system will automatically delete the applicable e-mails without the user's help. While certainly not perfect, it is likely less risky than the alternative. Of course, any decision to allow deletion of e-mail, whether manual or automatic has to be carefully done so as to ensure compliance with any discovery.

4. Get In Touch With Your Internal Systems

Does your company have one or multiple e-mail system platforms? If you have more than one, each one must be examined to determine what capabilities of space management they have. Are laptops being used? If so, there may be e-mails on the laptop that don't get deleted along with the e-mails on the desktop computer unless the user uses the "synchronize" function found in most e-mail software whenever the laptop is "docked." How will the policy apply to employees who work from home and store company e-mails on their home personal computer? Will you require them to run a periodic print out of their e-mails, will you exercise remote access, or will you just trust that they will comply on their own?

5. Raise Awareness of the Issues and Risks.

Make the appropriate decision makers[21] aware of the issue and risks associated with how e-mail is used and stored in your company[22]. If your company already has an e-mail retention policy, determine whether there is any meaningful compliance. If not, figure out why and try to address the issues.[23] If your company does not have an e-mail retention policy, work with the decision makers and create one that is reasonable

enough to be followed by employees, and easily implemented and enforced by your e-mail administrators.

6. Determine Potential Methods of Seeking Compliance.

Compliance with an e-mail policy can be obtained by automated monitoring of e-mail messages. Automated monitoring can be accomplished with readily available software, and most often with the e-mail software itself. For example, Microsoft® Exchange, a popular e-mail software program, can be programmed to automatically warn e-mail users when the user's allocated e-mail space has exceeded a specified size limit or if the user has e-mail that is older than a specified date, which date represents the end of the retention period. It can also be set up to automatically move messages older than a certain date to a designated folder for other treatment (such as further review) or automatically delete e-mail message that are older than a specified date. Other e-mail software, such as IBM's Lotus® Notes®, has similar capabilities.

While such software can be used as one component of an e-mail policy compliance plan, it is not a panacea. One major limitation of using software to warn, delete and manage e-mail is that its range is normally limited to the e-mail servers. Therefore, it cannot search, warn, delete or move e-mails if they are saved by users on their computer's local hard drive or floppy disk. Specific on-site audits would be necessary to scan messages not stored on the e-mail servers. If that is a concern at your company, consider including a prohibition in your policy against moving e-mails off of the e-mail servers.

In addition to automated enforcement methods to seek compliance, consider the old-fashioned written acknowledgment by employees. For example, consider requiring

that employees sign an annual statement that they are aware of the e-mail use and retention policies and of the ramifications for not complying. If desired, this can be packaged with other commonly used forms, such as annual conflicts of interest forms and other corporate compliance forms.

7. Communicate, Communicate, Communicate.

Design a communication, education and awareness campaign for the new policy. Assuming you have received approval, work with your information technology employees to design and implement a plan to communicate the policy to employees. If your company has an Intranet site and/or newsletter, consider including an article on the new policy. In the case of the Intranet site, hyperlink to the policy. Design a "Frequently Asked Questions" brochure and mail it to users, or post in on your company's Intranet, if one exists.

8. Choose a Retention Period and Compliance Method.

There are two main issues that you need to consider when designing a compliance plan - retention period and compliance method. First, it would be beneficial to determine what retention period will be long enough to gain compliance but short enough to meaningfully reduce the risks. For example, if a retention period is too short, there may be little or no compliance. A slightly longer period (e.g. 90 days versus 60 days) might help you achieve more compliance and therefore be more beneficial than a shorter period. Second, decide on a compliance method. Employees could be required to delete their own e-mails when older than the prescribed retention period and managers could be made responsible for their employees complying, or you could implement the automated method discussed earlier.

As an alternative, you might want to consider a middle of the road phased-in approach. For instance, use the first few months of the policy implementation to electronically warn e-mail users when they have e-mails that are older than the prescribed retention period, and remind them of their obligation to delete such e-mails. After some period of time and the completion of an education and awareness campaign, switch to the automated delete approach, giving them an electronic warning a few days or a week before the automatic deletion.

9. Conduct Training of Employees on The Use and Retention of E-Mail.

Make your employees aware of the risk of casual e-mails and of all aspects of your company's e-mail policy. E-mail users often believe that the messages they send and receive are private, and do not realize that such e-mails could come back to haunt the company (and them, potentially) in a lawsuit. Additionally, most users do not understand that deleted e-mail can often be restored from back-up tapes used by their company. Employees should be educated so that they can play a more active role in reducing the risk that e-mail content can lead to liability.

If you want to increase efficiency in training, consider packaging this training on e-mail retention with training on other electronic systems and software, such as Internet or Intranet use, word processing and other office software, or with the training on other policies. Also consider developing on-line training programs to minimize costs. Keep a "tips for e-mail users" brochure on-line or as a written brochure employees can refer to in the future.

10. Don't Forget to Cover New Employees.

Consider distributing the e-mail use and retention policy to new hires before they officially join your company. In addition, require them to sign a form that they acknowledge receipt of the policies and agree that they are required to read, understand and be bound by them. As an alternative, consider an automatic on-line training tool that requires first time e-mail users to read the policy and answer questions correctly before they qualify for e-mail access. Ask your information technology employees if they can create a user friendly but serious quiz. Either the form or on-line quiz will help ensure that new employees are not overlooked in your compliance plan. Once established, these approaches are relatively self-executing and are particularly useful in large companies and companies where turnover is high.

VII. Conclusion

Given the litigious culture in the United States, it is not likely a matter of whether your company will ever suffer the ill affects of e-mail discovery, but rather a matter of when.

E-mail discovery is becoming more common, and may soon be as common as paper discovery. Unless your company is willing to take the risk of spending unnecessarily large amounts on e-mail discovery compliance, potentially millions in damages or settlements of e-mail based lawsuits, and the corresponding bad publicity, it should have and enforce an e-mail use and retention policy. Having such policy will not prevent liability. However, if your company does not have one, the next time you are required to respond to e-mail discovery, you might wish it did.

[1] For example, an e-mail policy should state that employees are prohibited from using the company's e-mail systems to send potentially offensive jokes (which can be further defined, if desired); solicitations of any kind; chain mails; e-mails containing profane or abusive language; or any other e-mail that is not for legitimate business purposes. There can be a much longer laundry list of prohibited uses, depending on the level of specificity warranted.

[2] Whether compliance with an existing e-mail policy is not being monitored and enforced, or you are introducing a new policy, you need to determine whether and how compliance will be obtained and the ramifications for policy violations. Meet with your information technology experts together with your human resources department to determine what methods of monitoring are feasible, and what level of discipline is acceptable in your corporate environment.

[3] A much shorter period of time should be considered for retaining e-mails than paper documents, since e-mails are more likely to contain casual or non-business content.

[4] Automatic enforcement means the use of software to automatically warn of e-mails that are older than a certain date and/or automatically delete them.

[5] It is clear that companies are obligated to preserve e-mails (and other electronic and paper documents) once they are on notice of a litigation or formal investigation, and that indiscriminate destruction can bring about sanctions. However, this article does not delve into the dark depths of when the obligation to preserve evidence arises, and what constitutes negligent document destruction. Rather, it assumes that companies will be cognizant of the e-mail discovery obligation issue, and craft their e-mail retention policy to be consistent with such obligations.

[6] Having a general e-mail policy in which the e-mail retention policy is normally found, also helps manager the risks. The author strongly advocates having an e-mail policy but this article's focus is on e-mail retention.

[7] In re Brand Name Prescription Drugs Antitrust Litigation, 1995 WL 360526 (N.D. Ill. 1995) quoting Daewoo Electronics Co. v. United States. 650 F.Supp 1003, 1006 (Ct. Int'l Trade 1986).

[8] That number is not unreasonable given that many people with whom I have discussed this in real companies send and receive 50 or more per day. I would argue that over time, employees are becoming more sophisticated in technology usage and, therefore, the average number will go up over time.

[9] These numbers assume that all e-mail messages were saved and that the employees at E-mails Forever started with an empty e-mail "in-box" when they started counting e-mail volume.

[10] *Management: Managers Aren't Always Able to Get the Right Message Across with E-mail,* The Wall Street Journal, 8/6/96, page B1 (1996 WL-WSJ 3113477).

[11] *Judge Will Allow Race Evidence in King Case Hearing,* Los Angeles Times, 6/11/91, page 1, (1991 WL 2271569).

[12] Owens and Hutton v. Morgan Stanley. 1997 WL 793004 (S.O.N.Y. 1997) (not reported in F.Supp.).

[13] Id., pg. 2.

[14] *Morgan Stanley Employees Files Suit, Charging Race Bias Over E-Mail Jokes*, The Wall Street Journal, 1/13/97, page B8.

[15] *Morgan Stanley Settles Suit By Two Black Employees,* The Wall Street Journal, 3/2/98, page B8 (1998 WL-WSJ 3484561).

[16] U.S. v. Microsoft, Civ. Action No. 98-1232 (TPJ) D.C. May 18, 1998 Complaint at ¶17.

[17] An electronic filing cabinet is simply a filing system for e-mails on a computer generally through the use of customized file folders. Just like there is more than one system and are many options for filing paper documents in a physical file cabinet (e.g. alphabetically, by category, color coding, etc.), there can be multiple options for an e-mail or electronic (soft copy) document filing system on a computer.

[18] Allowing employees to save drafts (including documents containing revision marks), may also create unnecessary risk. Additionally, allowing employees to save electronic documents wherever they want on their computer (e.g. floppy disk or local hard drive) may increase the costs of discovery since such documents may be outside of the scope of document location software and will make it harder for your company to locate important documents when responding to discovery or any other time, especially when an employee with their own electronic filing system leaves.

[19] An e-mail retention policy is often contained in general e-mail use policy, but can be contained in a paper document retention policy.

[20] Computer disk space is usually dedicated for e-mail storage and related treatment. Such space generally includes an "in-box," "out-box," "sent" box and "deleted" box.

[21] In some companies, the CIO may be the ultimate decision maker. In smaller companies, it may be the e-mail administrator, CEO, general counsel or other manager.

[22] If your company does not already have an e-mail policy, this would be a good opportunity to discuss the merits of having one and begin the drafting process.

[23] For example, perhaps your company has a policy that has not been communicated well enough and few employees are aware of its existence, maybe your company's e-mail administrators do not have the tools to monitor or delete e-mails, or have not been given the appropriate authority to do so, or maybe your current e-mail retention period is too short for your company's needs, and therefore the employees are willfully disregarded it. Increasing the retention period (e.g. from 30 to 60 days) might gain compliance and it would be less risky to have a sixty (60) day e-mail retention period that employees are, for the most part, complying with than to have a thirty (30) day retention period that nobody follows.

Preventative Law:

How to Raise the Legal Awareness of Your Employees.

Presented by

Darity Wesley

ACXIOM® DataQuick Property Data & Products

dwesley@dataquick.com
San Diego, CA
November, 1999

Educate Yourself/ Know Your Company

- Company or Division's Business Processes.
- Who does What, How & Why?
- Analyze exposure Areas.
- Strategies.
- Garner Support.
- Make a Plan.

Human Resources: Training

- Educate your leaders.
- Do not rely completely on HR Personnel.
- Train your HR Personnel to the company culture/perspective.

Human Resources: Training cont.

- **Know particular legal employment issues for your company.**
  - Safety
  - Worker's Comp
  - Labor/Union
  - Americans with Disabilities Act
  - EEOC Issues
  - Exempt/Non-Exempt
  - Sexual Harassment
  - AD Nausem
- **Have an open door policy.**

Sales Training

- Contractual issues
- Misrepresentation issues
- Anti-Trust issues

Customer Support Training

- **Education**
  - **Specific areas to address regarding your business.**
  - **General legal theories.**
  - **Documentation of problems.**

Technology/Developers

- Internet Issues
- Manufacturing Issues
- Intellectual Property Issues
- Clearances
- Licenses
- Alpha/Beta Testing Issues

Marketing Communications

- Review all Press Releases.
- Review all Informative Communications to Customers and Employees.
- Review All Marketing Materials.
  - Representations about Products.
  - Trademarks and Copyrights.

New Hire Orientation

- Make them aware you are there, available, ready to answer questions.
- Privacy/suppression issues.

Preventative Law Guide Lines:

- Analyze exposure areas.
- Educate leaders, teams, departments, about how to avoid creating problems.
- Get peripherally involved at all levels of your company.
- Convey information to all levels of your organization.
- Don't be shy - US?
- Keep an open door.
- Be accessible.