State of North Carolina
Office of Information Technology Services

Privacy and Classification of Information

Presented by: Sam Byassee

ITS General Counsel

sam.byassee@its.nc.gov

North Carolina Digital Government Summit

North Raleigh Hilton

September 3-4, 2008

Agenda

- Classifying Electronic Information
- Storing & Maintaining Electronic Information
- Securing Electronic Data
  (and Dealing with a security breach)
- Questions

DISCLAIMER

You may think you understand what you believe I said, but what you heard was not what I meant.

- This is a discussion about general principles – application always depends on the specific facts of a situation.
- It’s my opinion and you’re welcome to it.
- Ask your legal advisor.

Classifying Electronic Data

- Is it a public record?
- Is it confidential?

A Purely Hypothetical Situation

A state employee communicates using e-mail. Messages include:

- Specific projects - draft reports, information exchange, opinions, meeting notes, status reports, meeting notes, inquiries (either created or received)
- Agency materials – announcements, meeting schedules, policies, standard reports, events, requests for information
- Non-business – lunch plans, comments about events, personal inquiries, e-mail with friends/family, Spam

Hypothetical Situation, cont.

- Employee is told to delete unnecessary e-mail concerning a particular issue
- Clean out both Inbox and Deleted Items folder
- Employee follows instructions
- For some reason, newspaper makes records request for employee's e-mail messages on that particular issue

What do you do?

a) Report that the employee never uses e-mail because they are allergic to electrons;

b) Tell the employee to go re-create all of the e-mail that he/she can recall about the relevant issue;

c) Check to be sure no other employee has any embarrassing e-mail relevant the record request;

d) Inform the newspaper that electronically-maintained information doesn't count as a record.

N.C. Public Records Act

G.S. Chapter 132

"Public record" shall mean **all documents**, … magnetic or other tapes, electronic data-processing records, … **regardless of physical form** or characteristics, made or received pursuant to law or ordinance in connection with the **transaction of public business** by any … public office, public officer or official, … institution, board, commission, bureau, council, department, authority or other unit of government of the State or of any county, unit, special district or other political subdivision of government.

[§132-1(a)]

Access to Public Records

- The public records … of North Carolina government or its subdivisions are the **property of the people**. Therefore, it is the policy of this State that the **people may obtain copies** of … public records … free or at minimal cost.
- "minimal cost" shall mean the actual cost of reproducing the public record.

[§132-1(b)]

Exceptions

- Confidential Information (mostly privately-owned trade secrets)
- Certain criminal investigation-related information
- Emergency response plans, public security information, 911 ID data
- *Personal Identifying Information*
- Attorney communications and trial prep materials

[§132-1.2 to -1.10]

Access to Electronic Records

- Every custodian of public records shall permit any record … to be inspected and examined at reasonable times and under reasonable supervision by any person [without requiring disclosure of the purpose of the request].
- furnish copies … upon payment of any fees … prescribed by law.
- "custodian" does **not** mean an agency that holds the public records of other agencies solely for purposes of storage or safekeeping.

[§132-6]

Access Conditions

- Cannot refuse access because confidential information intermingled – must redact (at agency's cost).
- Public may choose format in which record is to be produced.
- Agency must provide fields and record layout information for database compilations.
- Agency is **not** required to create records it does not possess.

Fees for Making Copies

- “actual cost" is limited to direct, chargeable costs of reproducing the record as determined by generally accepted accounting principles.
- Excludes costs that would have been incurred by the agency even if a request to copy the record had not been made.
- If the request requires **extensive use** of information technology resources or **extensive clerical or supervisory assistance** by personnel of the agency involved, … then the agency may charge, in addition to the actual cost of duplication, a **special service charge**, which shall be reasonable and shall be **based on the actual cost incurred** for such extensive use of information technology resources or the labor costs of the personnel providing the services.

[§132-6.2]

Keeping Public Records

- Nothing in North Carolina law requires that a public record – electronic or otherwise – be retained forever.

- Procedures for the retention, maintenance and disposal of public records are administered by the Department of Cultural Resources

Records Maintenance Principles

- How long to maintain a record prior to disposal?
- Who makes the decision?
- How should electronic records be maintained?

  (Hint: Back-up is not an archive.)

Maintenance Considerations

- Cost of maintenance and retrieval
- Ease of retrieval
- Accuracy of retrieval
- Ease of disposal
- Electronic discovery issues
- Public Access considerations

Security

- State CIO responsible for setting statewide technical standards for information security [posted at: http://www.scio.nc.gov/sitPolicies.asp].
- Security policies and standards administered by ITS' Enterprise Security and Risk Management Office (ESRMO)

  [contact Ann Garrett - ann.garrett@its.nc.gov]
- All security incidents to be reported to ESRMO

Personal Identifying Information

- “Personal information” includes a person's first name or initial, **plus** last name, **in combination with** various types of identification numbers, account numbers, PINs, etc., including a catch all "any other numbers or information that can be used to access a person's financial resources."
- Thus, PII generally includes information that not only allows a person to be identified, but that also tends to assist someone else in assuming that person's identity or to access financial or private information.

See G.S. §75-66

PII Definition

The term "identifying information" as used in this Article includes the following:

(1) Social security or employer taxpayer identification numbers.
(2) Drivers license, State identification card, or passport numbers.
(3) Checking account numbers.
(4) Savings account numbers.
(5) Credit card numbers.
(6) Debit card numbers.
(7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).
(8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
(9) Digital signatures.
(10) Any other numbers or information that can be used to access a person's financial resources.
(11) Biometric data.
(12) Fingerprints.
(13) Passwords.
(14) Parent's legal surname prior to marriage.

See G.S. §14-113.20

Exclusion from PII

- Any information in "publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, **including name, address and telephone number**..."

See G.S. §75-61

Security Breach

- "Security breach" – An **incident of unauthorized access to and acquisition of** *unencrypted and unredacted* records or data containing personal information …
- where illegal use of the personal information has occurred **or** is reasonably likely to occur **or** that creates a material risk of harm to a consumer.
- Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach.

See §75-61(14)

Notice to Affected Persons

Clear and conspicuous, and shall include a description of the following:

(1) The incident in general terms.

(2) The type of personal information that was subject to the unauthorized access and acquisition.

(3) The general acts of the business to protect the personal information from further unauthorized access.

(4) A telephone number that the person may call for further information and assistance, if one exists.

(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

If more than 1,000 affected persons, notice to Atty. Gen.

Methods of Notice

(1) Written notice.

(2) Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically if the notice provided is consistent with … 15 U.S.C. § 7001.

(3) Telephonic notice provided that contact is made directly with the affected persons.

(4) Substitute notice (depending on expense and/or lack of adequate contact information)

See §75-65

QUESTIONS ?

William Sam Byassee

N.C. Office of Information Technology Services

919-754-6670

sam.byassee@its.nc.gov

Thank You