KENTUCKY DEPARTMENT FOR LOCAL GOVERNMENT

Protection of Personal Information

October 4th

Covington, KY

Darren T. Sammons, Staff Attorney,
Department for Local Government
(502) 573-2382

"It used to be expensive to make things public and cheap to make them private. Now it's expensive to make things private and cheap to make them public."

Clay Shirky,

Professor, N.Y.U.

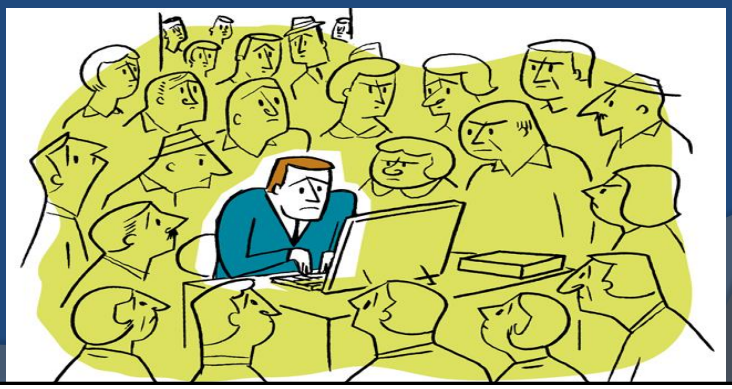
" Privacy is not for the passive."

Jeffrey Rosen,

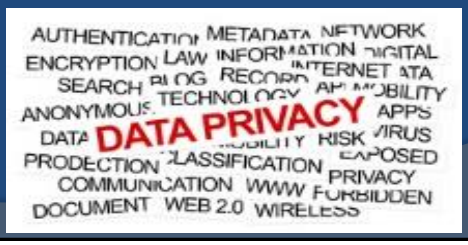
Professor of Law

George Washington University

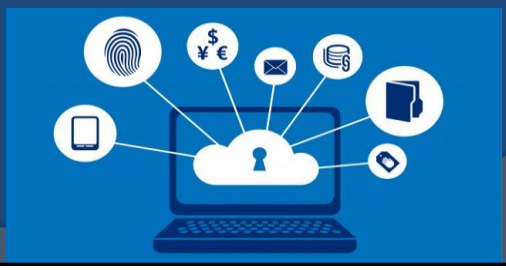
“ There are no secrets better kept than the secrets that everybody guesses.” George Bernard Shaw



“ In view of all the deadly computer viruses that have been spreading lately, Weekend Update would like to remind you: when you link up to a computer, you’re linking up to every computer that computer has ever linked up to.” Dennis Miller



"A computer lets you make mistakes faster than any invention in human history—with the possible exceptions of handguns and tequila." Mitch Ratliff



KRS 61.931 through .934

- Promulgated by the Kentucky General Assembly as House Bill 5 in 2014
- Goal: To Protect Personal Information and Establish Framework for Reporting Breaches

What is personal information?

A name or similar identifying info.

+

Account #s or Gov't Issued #s/Info, or Healthcare information

(My Definition)

What did 2014's HB 5 do?

- First, it defined Personal Information as "an individual's first name, or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

- (a) An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
- (b) A social security number;
- (c) A taxpayer identification number that incorporates a Social Security number;
- (d) A driver's license number, state identification card, or other individual identification number issued by any agency.

- (e) A passport number or other identification number issued by the U.S. government; or
- (f) Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.

What did 2014's HB 5 do?

- It defined Public Record as:
- "all books, PAPERS*, maps, photographs, cards, tapes, disks, diskettes, recordings, and OTHER DOCUMENTARY MATERIALS, regardless of physical form or characteristics, which are prepared, owned, used, in the possession of, or retained by a public agency." KRS 61.931(7)(a)
- *This is not just "Cyber Security".

What is a "Public Agency"?

- The State level Executive Branch
- Every: county, city, municipal corporation, urban-county government, charter county government, consolidated local gov't, and unified local gov't.; KRS 61.931(1)(a) & (b)

and

Public Agency (cont.)

- "Every organizational unit, department, division, branch, section, unit, office, administrative body, program cabinet, bureau, board, commission, committee, subcommittee, ad hoc committee, council, authority, public agency, instrumentality, interagency body, special purpose governmental entity, or public corporation of an entity specified in paragraph (a) or (b) of this subsection or created, controlled, etc. by an entity specified in (a) or (b) of this subsection." KRS 61.931(1)(c).

My definition of Agency for our purposes:

"Pretty much every form of local governmental entity."

What did 2014's HB 5 do?

- It required the Department for Local Government to develop policies regarding "reasonable security and breach investigation procedures and practices" for units of local government.

In response, DLG developed policies as the law required.

- DLG's policies are available as a downloadable .pdf on our website at:
- https://kydlgweb.ky.gov/Documents/Legal/InformationSecurityPoliciesProcedures.pdf

(Just go to our homepage, and then select "Legal" on the right-hand side and then you'll see a link).

What does DLG's Policy say?

- "Media containing personal information shall be physically controlled and securely stored in a manner meant to ensure that the media cannot be accessed by unauthorized individuals. This may require storing media in locked containers such as cabinets, drawers, rooms, or similar locations if unauthorized individuals have unescorted access to areas where personal information is stored." (Cont.)

DLG's Policy (Cont.)

- "If personal information is stored in an electronic format, it shall be protected from access by unauthorized individuals. Such information must be protected by software that prevents unauthorized access. If personal information is transmitted via e-mail or other electronic means, it must be sent using appropriate encryption mechanisms."

Point of Contact

The Entity shall designate a Point of Contact ("POC"). The POC shall serve the following functions:

1) Maintain The Entity's Information Security Policy and be familiar with its requirements;

2) Ensure The Entity's employees and others with access to personal information are aware of and understand the Information Security Policy;

3) Serve as contact for inquiries from other agencies regarding its Information Security Policy and any incidents;

4) Be responsible for ensuring compliance with the Information Security Policy; and

5) Be responsible for responding to any incidents.

- DLG's Policy addresses software and encryption issues.
- Recommend the policy be reviewed by policymakers and information technology employees and contact DLG or COT with questions.

- The level of protection afforded by security software should be commensurate with the sensitivity of the data.

- Systems, networks and application software used to process personal information must adhere to the highest level of protection reasonably practical.
- Local Gov’ts shall use Intrusion Detection and Prevention software approved by COT. **A list of approved software is available on the COT website**.
- As an alternative, LGUs may use software not approved by COT, provided that such software provides comparable, or superior, protection.

- Only authorized individuals are permitted access to media containing personal information. In addition to controlling physical access, user authentication should provide audit access information*. Any access must comply with applicable regulatory requirements.

*In other words, there should be a way to track who accessed what.

Physical Security Procedures

- Given the broad variety of sizes and types of LGUs, each will have different security challenges and resources available to address those challenges. This policy does not specifically address physical security needs and threats, such as natural disasters, electrical outages, fire, or other physical threats to personnel or information resources. LGUs are responsible for establishing and maintaining their own physical security procedures.

Physical Security (cont.)

- There is no "one size fits all" approach to physical security.
- In general, use common sense methods to restrict access to personal information. Lock it up, keep in a locked room, etc.

Non-digital media

- Local Gov’ts shall secure and, when applicable, appropriately dispose of non-digital media. Non-digital media containing personal information must be properly stored and secured from view by unauthorized persons.
- Secure measures must be employed by the Local Gov’t and all permissive users to safeguard personal information contained on all Local Gov’t technology resources.
- Local Gov’ts shall ensure that all authorized personnel are familiar with and comply with the Information Security Policy. Local Gov’ts shall ensure that only authorized personnel may hold and have access to personal information.

Portable Computing Devices

- This policy prohibits the unnecessary placement (download or input) of personal information on portable computing devices.
- If you do, be aware of the risks.
- Portable devices pose all the problems of both physical and electronic personal information—and require both physical control and encryption.
- Best practice is to try to minimize the amount of personal information you keep on a portable device.

Types of Incidents

- Threats to the security of personal information arise in many different ways. Local Governments are encouraged to be aware of the different types of threats and to enact reasonable measures to protect against each. Attacks on personal information may arise from:

- External/Removable Media—an attack executed from removable media (e.g. flash drive, CD) or a peripheral device.
- Attrition—An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.
- Web—An attack executed from a website or web-based application.
- Email—An attack executed via an email message or attachment.

- Improper usage—Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.
- Loss or Theft of Equipment—The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.
- Other—an attack that does not fit into any of the other categories.

Destruction of Records Containing Personal Information

- Have a document retention policy (and follow it).
- Use appropriate methods to destroy personal information:

- Hire a document disposal contractor to dispose of the material. The contractor should be certified by a recognized trade association and should use disk sanitizing software and/or equipment approved by the United States Department of Defense. The Local Government should review and evaluate the disposal company's information security policies and procedures. The Local Government should review an independent audit of a disposal company's operations and/or its compliance with nationally recognized standards.

- Secure and use shredding equipment that performs cross-cut or confetti patterns.
- Secure and use disk sanitizing or erasing software or equipment approved by the United States Department of Defense.
- Modify the information to make it unreadable, unusable or indecipherable through any means.

Reporting a Breach

- When a LGU identifies that a security breach has occurred in which personal information has been disclosed to, or obtained by, an unauthorized person, within three business days it shall notify Kentucky State Police, the Auditor of Public Accounts, the Attorney General and the Commissioner of the Department for Local Government and complete form COT-F012. The LGU shall document the following:

Reporting a Breach (cont.)

- Each Local Government must disclose a security breach in which personal information is disclosed to, or obtained by, an unauthorized person.
- Notification of the incident must be made in the most prompt and expedient manner after the incident has been discovered.
- Within thirty-five days, a letter notifying affected individuals of actual or suspected loss or disclosure of personal information must be sent by the LGU describing the types of information lost and recommended actions to be taken to mitigate the potential misuse of their information.

Reporting a Breach (cont.)

- Document the following:
- 1) Preliminary Reporting and description of the incident;
- 2) Response, including evidence gathered;
- 3) Final Assessment and corrective action taken; and
- 4) Final Reporting

- Incident Response procedures can be a reaction to security activities such as:
- 1) Unauthorized access to Personnel, Data, or Resources;
- 2) Denial of Service Attacks;
- 3) Actual or Anticipated Widespread Malware Infections;
- 4) Data Breaches;

- 5) Loss/Theft of Equipment;
- 6) Significant Disruption of Services
- 7) Significant Level of Unauthorized Scanning Activity to or from Hosts on the Network

- Investigation: Local Governments shall make reasonable efforts to investigate any security breaches in which personal information is disclosed to, or obtained by, an unauthorized person and shall take appropriate corrective action.

- LGUs must comply with all federal and state laws and policies for information disclosure to media or the public. In some circumstances, communication about an incident is necessary, such as contacting law enforcement. LGUs should use discretion in disclosing information about an incident.

- Within the parameters of the law, minimal disclosure regarding incidents is preferred to prevent unauthorized persons from acquiring sensitive information regarding the incident, security protocols and similar matters, in an effort to avoid additional disruption and financial loss.

Summary:

- Remember, not all information is "personal information."
- If it is on a computer, use appropriate protection software.
- If it is in a physical format, limit access using appropriate controls.
- If there's a breach—report it!

Questions?

Darren Sammons
Staff Attorney
Department for Local Government
(502) 573-2382


DLG
DEPARTMENT
FOR LOCAL
GOVERNMENT