

CURRENT AND EMERGING PRIVACY LAW

BRYAN WISE

**TAFT, STETTINIUS & HOLLISTER
LLP**

OVERVIEW

- State Law
 - Ohio H.B. 104
- Federal Laws
 - Gramm-Leach-Bliley Act
 - HIPPA
 - FCRA/FACT Act
 - COPPA
 - CAN-SPAM Act
 - Posting of Privacy Policies (California law)
 - Others which may affect privacy practices

Overview (Cont'd)

- Future Federal Legislation
 - Protecting Children in the 21st Century Act
 - Protecting Consumer Phone Records Act
 - H.R. 964 – Unfair/Deceptive Practices Involving Computer
 - Proposed Social Security Number Protection Bills
 - H.R. 836 – Security Breach Notification Bill
 - H.R. 1015 – Auto dealers disclosure of “black boxes” and consumer right to opt out
- Resources for Information on Privacy Laws

OHIO H.B 104

- Put into effect in 2006
- Requires any entity with computerized data containing personal information to expeditiously notify Ohio residents whose personal information was accessed or may have been accessed by security breaches
- Regulates state agencies, governmental bodies and "persons" (includes business entities)
- Will focus on requirements of "persons" here

Ohio H.B. 104

Definition of "Person"

- Places reporting obligations on any "person" (which includes business entity that conducts business in Ohio) who:
 - Owns or licenses computerized data containing specified personal information; or
 - On behalf of or at the direction of another person or governmental agency is the custodian of or stores computerized data containing specified personal information

Ohio H.B. 104 – Notification Obligations

- Requires any “person” to disclose any breach of the security of its system to any Ohio resident:
 - Whose personal information was, or reasonable is believed to have been, accessed and acquired by an unauthorized person;
 - If the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or fraud.

Ohio H.B. 104 – Notification Time Period

- Ohio H.B. 104 requires different notification periods for types of “persons”
 - *Own or license computerized data* – “in the most expedient time possible, but not later than 45 days following its discovery or notification of the breach to the security system”
 - *Custodian or Storer on behalf another person or a governmental entity* – “in an expeditious manner”

Ohio H.B. 104 – Permissible Delay of Notification

- A “person” may delay the required notification if a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security.

Ohio H.B. 104 – Methods of Notification

- Permissible methods of notification include:
 - Written Notice
 - Electronic Notice
 - IF the person's primary method of communication with the resident is by electronic means
 - Telephone Notice
 - Substitute Notice
 - IF certain qualifications are met
 - Two forms of substitute notice depending on which circumstances apply

Ohio H.B. 104

Substitute Notice

- First form – R.C. § 1349.19(E)(4)
 - If the person does not have sufficient contact information for the residents; OR
 - If the cost of providing notification by these methods exceeds \$250,000; OR
 - The number of residents exceeds 500,000.
- Then Substitute Notice MAY be provided.

Ohio H.B. 104

Substitute Notice (cont'd)

- In this situation, Substitute Notice entails **ALL** of the following:
 - Electronic mail notice if the person has an electronic mail address for the resident to whom the disclosure must be made;
 - Conspicuous posting of the disclosure or notice on the person's website, if the person maintains one; AND
 - Notification to major media outlets
 - To the extent that the total readership, viewing audience and listening audience of all of the outlets notified equals or exceeds 75% of the population.

Ohio H.B. 104

Substitute Notice (cont'd)

- Second Form – R.C. § 1349.19(E)(5)
 - If the person is a business entity with 10 employees or fewer **AND**
 - The cost of providing notice will exceed \$10,000
 - Then Substitute Notice may be provided.

Ohio H.B. 104

Substitute Notice (cont'd)

- Substitute Notice in this situation entails **ALL** of the following:
 - Notification by paid advertisement in a local newspaper that is distributed in the geographic area in which the business entity is located;
 - Must take up at least $\frac{1}{4}$ of a page;
 - Must be published at least once a week for three weeks;AND
 - Conspicuous posting of the disclosure or notice on the business entity's website, if the business entity maintains one; AND
 - Notification to major media outlets in the geographic area in which the business entity is located

Ohio H.B. 104

"Quick Hits"

- "Financial Institutions," "Trust Companies," "Credit Unions" or any of their "affiliates" with federal reporting requirements are exempt from the reporting requirements of R.C. § 1349.19
- Residents of Ohio cannot waive the notice requirements
- If the breach of a single occurrence requires disclosure to more than a thousand Ohio residents, the person must also notify all consumer reporting agencies (i.e. credit bureaus) of the timing, distribution and content of the disclosure.
- The attorney general may conduct investigations and bring a civil lawsuit upon an alleged failure to comply with these requirements.

FEDERAL PRIVACY LAW – GRAHAM-LEACH-BLILEY ACT (GLB)

- GLB Act requires a “financial institution” to:
 - Provide notice to “consumers” and “customers” about the institution’s practices in collecting, using and disclosing “nonpublic personal information” about them.
 - Provide “consumers” and customers an opportunity to object to disclosure of their “nonpublic information” to “nonaffiliated third parties” (“opt out” provisions)
 - Prohibits third party receiving NPI from a financial institution from disclosing it
 - outside of statutory exception or
 - outside the scope of terms of financial institution’s privacy notice
- BROAD SCOPE of information covered: “Any” personally identifiable information
 - For example, customer name and address lists included

GLB Act – “Financial Institutions”

- Act has broad definition of FIs
 - Banks, credit unions, etc.
 - Also includes debt collectors, insurance companies, securities brokers, retailers that use own credit cards, tax preparation services, check printers, and automobile leasing companies
- Agents of financial institutions not included

GLB Act – “Consumers” and “Customers”

- “Consumer” and “Customer” describe the type of relationship an individual has with the financial institution
 - “Consumer” is a person who obtains a financial product or service to be used primarily personal or household purposes
 - “Customer” is a consumer who has a continuing relationship with a financial institution, and includes former and lapsed customers
- GLB Act has different protections for each type of relationship

GLB Act

Notice Requirements

- Appearance must be clear and conspicuous
- Must contain certain mandatory disclosures
- Must be delivered in a manner “reasonably expected to be received”
 - May be posted on website, but there are special rules which must be followed
- Initial and annual notices
 - Requirements differ between consumers and customers¹⁸

GLB Act

Opt Out Requirement

- Must provide notice and opportunity to opt out prior to any disclosure
 - Obligation continues throughout relationship
 - Reasonable opportunity to opt out
 - Must provide 30 days to customer to opt out after notice sent
- Exceptions to Opt Out Requirement
 - Necessary to process or service transaction
 - Protect record security and confidentiality
 - Respond to requests from regulators, self-regulatory organizations (SROs), and law enforcement
 - Provide information to legal counsel and entities assessing compliance with industry standards
 - Reports to credit bureaus
 - Fraud protection
 - Comply with laws and legal process
 - In connection with proposed or actual merger
 - Parties hold legal interest relating to consumer
 - Third party performance of services for or on behalf of financial institution (still required to provide initial notice)

FEDERAL PRIVACY LAW – FCRA AND FACT Act

- Fair Credit Reporting Act was amended in 2003 as the “Fair & Accurate Credit Transactions Act” (FACT Act)
- Regulates “consumer reporting agencies” (CRAs), “users” and “furnishers”
- FCRA applies only to “consumer reports”
 - Three part test:
 - Personally identifiable data that bears on 1 of 7 statutory factors
 - Used or collected for permissible purpose
 - Communicated by a CRA
- FACT Act: Special notice and opt-out rules for use in marketing and solicitations

FCRA and FACT Act

Duties of Entities

■ Duties of CRAs

- Provide reports for “permissible purposes”
- Ensure that data is reasonable accurate and current
- Furnish consumer with copy of consumer report
- Investigate alleged inaccuracies and correct, if necessary
- Must place fraud alert on credit file if requested by consumer

■ Duties of Others

- Users prohibited from procuring reports for non-permissible purposes
- Users prohibited from using or disclosing reports for purposes other than for the purpose for which they were produced
- User must notify consumer of identity of CRA providing info
- Furnishers must investigate if consumers dispute accuracy

FEDERAL PRIVACY LAW - HIPAA

- Health Insurance Portability & Accountability Act (HIPAA)
- Basic Rule: Unless explicitly exempted by HHS, no directly regulated entity can access, use or disclose individually identifiable health information without first obtaining the informed and written permission (“authorization”) of the affected individual.
- Rule applies directly to:
 - Health Care Providers who transmit individually identifiable health information in electronic form
 - Health Plans
 - Health care clearinghouses

HIPAA – “BUSINESS ASSOCIATES”

- Generally, the definition of a “business associate” involves performing some function or services for a covered entity.
- Rule can affect “business associates”, which may include:
 - Direct marketers
 - Pharmaceutical manufacturers
- General Rule:
 - Without prior authorization, a covered entity may disclose protected health information to a BA, and may allow that BA to create or receive protected health information on its behalf, IF the covered entity obtains satisfactory assurance that the BA will appropriately safeguard the info.

HIPAA – INFORMATION PROTECTED

- “Protected Health Information” is all individually identifiable health information that:
 - Is created or received by a covered entity;
 - Relates to the past, present or future physical condition of an individual; to the provision of health care to an individual; or to payment for provision of health care to an individual;
 - Identifies the individual
- Data which IDs individuals include:
 - Name
 - Geographic subdivisions smaller than a state
 - Dates (except year) of treatment, birth, death, admission, etc.
 - Telephone numbers
 - Social security or medical record numbers
 - Photographs
- Clear, informed written permission required before disclosure (clear elements which must be satisfied)

FEDERAL PRIVACY LAW – COPPA

- Children's Online Privacy Protection Act
- Applies to the collection of personal information from children under the age of 13
- Rules set out:
 - What a website operator must include in a privacy policy;
 - When and how to seek verifiable consent from a parent; and
 - What responsibilities an operator has to protect children's privacy and safety online

COPPA – WHO MUST COMPLY?

- An operator of a commercial website or an online service directed to children under 13 that collects personal information from children; OR
- An operator of a general audience website and have actual knowledge that you are collecting personal information from children

COPPA – “Operator” and “Directed at Children”

- To determine whether an entity is an “operator,” the FTC will consider:
 - Who owns and controls the information;
 - Who pays for the collection and maintenance of the information;
 - What the pre-existing contractual relationships are in connection with the information; and
 - What role the website plays in collecting or maintaining the information.
- To determine whether a website is “directed at children,” the FTC will consider:
 - The subject matter
 - Visual or audio content
 - Age of models on site
 - Language
 - Advertising directed to children
 - Use of animated characters or other child-oriented features

COPPA – Requirements on Operators

- Under COPPA, Operators must:
 - Post a privacy policy
 - Provide parental notice of privacy practices
 - Obtain verifiable parental consent before collecting, using or disclosing personal information from a child.
 - Certain exceptions apply
 - Provide parental access to children's information and opportunity to opt out of future collection
 - Provide parents the option to agree to the collection and use of child's personal information without agreeing to the disclosure to third parties
 - Provide new notice for consent if policies change
 - Ensure confidentiality, security and integrity of personal information collected
 - Limit collection to what is reasonable necessary to participate

COPPA – Safe Harbors

- In its enforcement of COPPA, the FTC does allow for industry groups to create self-regulatory programs to govern compliance.
- If the FTC approves the compliance plan of the industry group, then an operators compliance with the self-regulatory guidelines will generally serve as a safe harbor in any enforcement action for violations of the Rule.
- Check with the appropriate industry group to see if they have a FTC-approved plan.

Federal Privacy Law – CAN-SPAM Act

- CAN-SPAM regulates commercial e-mail messages (CEMs)
 - Does not bar them completely
 - Sets rules for sending them
- Brief Overview:
 - No false or misleading header info
 - No deceptive subject lines – must indicate commercial nature
 - Must provide opt-out method and honor within 10 business days
 - Must include senders valid postal address

Posting of Privacy Policies

- Most websites voluntarily post a privacy policy, which means they have to conform to laws against deceptive practices (both state and federal, i.e. Section 5 of the FTC Act)
- California law has become the de facto national standard to the extent that a website anticipates collecting data from California residents

Posting of Privacy Policy

- California's Online Privacy Protection Act requires companies using web sites to collect personally identifiable information to:
 - Identify the categories of PII collected through the website
 - Identify the categories of third-party entities or persons with whom the PII may be shared
 - If you allow review and changes of PII, explain how a consumer can do so
 - Explain how consumers can learn of changes to privacy policy
 - Identify effective date of privacy policy

Other Federal Laws which may affect Privacy Laws

- USA PATRIOT Act
 - What information certain governmental entities may obtain
- E-SIGN Act
 - Essentially, gives same legal effect to electronic records/contracts/signatures as paper records/contracts/signatures
- Driver's Privacy Protection Act
 - Governs release of driver's license records by state departments of motor vehicles

Federal Legislation on the Horizon

- There have been several new privacy bills introduced into Congress this year.
- Protecting Children in the 21st Century Act
 - Prohibits the purchase or sale of personal information of individuals who are known to be under the age of 16 for the purposes of marketing.

Federal Legislation on the Horizon

- Protecting Consumer Phone Records Act
 - Prohibits providers of commercial mobile services from providing wireless phone numbers to directories without notice and consent
- H.R. 964
 - Criminalizes unfair/deceptive practices involving computers, including accessing or hijacking another's computer to damage it

Federal Legislation on the Horizon

- Proposed Social Security Number Protection Bills
 - Two bills in the House and one in the Senate aiming to protect SSNs
 - H.R. 220 would prohibit the establishment in the Federal Government of any uniform national identifying number.
 - H.R. 948 and S. 238 would prohibit the display, purchase or sale of SSNs altogether

Federal Legislation on the Horizon

- H.R. 836 – Security Breach Notification Bill
 - Cyber-Security Enhancement and Consumer Data Protection Act of 2007
 - Provides notification requirements for breaches of security
 - May nationalize the various state bills
 - Includes criminalization for failure to disclose
- H.R. 1015 – Auto dealers
 - Requires automobile dealers to disclose to consumers the presence of “black boxes” (event data recorders) on new automobiles;
 - Also requires manufacturers to provide the consumer with the option to enable or disable such devices on future automobiles

Some Research Websites Regarding Privacy Legislation

- Federal Trade Commission – www.ftc.gov – gives advice on how to comply with a number of the laws discussed
- THOMAS – Library of Congress – thomas.loc.gov
- Electronic Privacy Information Center (EPIC) – www.epic.org
- International Association of Privacy Professionals – www.privacyassociation.org
- National Conference of State Legislators – www.ncsl.org
- Compuworld newsletters – www.compuworld.com
- Hudson Cook – consumer finance issues and issues that would be of interest to car dealers
- Privacy.org – lots of news and information on both the national and international front

QUESTIONS?

- THANK YOU
- Questions after session:
Bryan Wise
Taft, Stettinius & Hollister LLP
wise@taftlaw.com
(513) 381-2838