US Cybersecurity Legislation – Part 2

Federal Trade Commission Act
And the Federal Trade Commission

I did a Google search on “cybersecurity laws” and this came up:

The primary law governing cybersecurity in the United States is the ***Federal Trade Commission Act (FTCA)****. This law prohibits deceptive acts and practices in business, including those related to data security*

The Federal Trade Commission Act was signed into law by President Herbert Hoover in 1914 (and amended in 2006), some 80+ years before we even knew what cybersecurity was. So what does it have to do with cybersecurity?

Federal Trade Commission Act

- The key provision of the Federal Trade Commission Act is to establish the Federal Trade Commission (FTC)
- The Federal Trade Commission Act empowered the FTC to:
  - Prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce;
  - Seek monetary redress and other relief for conduct injurious to consumers;
  - Prescribe rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices;
  - Gather and compile information and conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and
  - Make reports and legislative recommendations to Congress and the public. A number of other statutes listed here are enforced under the FTC Act

Federal Trade Commission

- Enforce a variety of antitrust and consumer protection laws affecting virtually every area of commerce, with some exceptions concerning banks, insurance companies, non-profits, transportation and communications common carriers, air carriers, and some other entities The agency leverages its resources and targets its enforcement efforts at practices that cause the greatest harm to consumers.
- Investigate and prevent unfair methods of competition, and unfair or deceptive acts or practices affecting commerce
- Seek relief for consumers, including injunctions and restitution, and in some instances to seek civil penalties from wrongdoers
- Implement trade regulation rules defining with specificity acts or practices that are unfair or deceptive
- Publish reports and make legislative recommendations to Congress about issues affecting the economy
- Enforce various antitrust laws under Section 5(a) of the FTC Act as well as the Clayton Act. The FTC monitors all its orders to ensure compliance
- The FTC conducts regular reviews of all its rules and guides on a rotating basis to make sure they are up-to-date, effective, and not overly burdensome

Federal Trade Commission and Cybersecurity Standards for Safeguarding Customer Information

- Under Title 16 — Commercial Practices Chapter I —Federal Trade Commission, Subchapter C —Regulations Under Specific Acts of Congress, Part 314
- Applies to the handling of customer information by all financial institutions over which the FTC has rulemaking authority pursuant to section 501(b) of the Gramm-Leach-Bliley Act
- Requires financial institutions to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue
- The information security program shall:
  - Ensure the security and confidentiality of customer information;
  - Protect against any anticipated threats or hazards to the security or integrity of such information; and
  - Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer

Federal Trade Commission and Cybersecurity Standards for Safeguarding Customer Information

Elements of the Information Security Program

- Designate a qualified individual responsible for overseeing, implementing and enforcing the information security program
- Base information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information
- Design and implement safeguards to control the risks identified through risk assessment – includes requirement to "Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest"
- Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures
- Implement policies and procedures to ensure that personnel are able to enact your information security program
- Oversee service providers
- Evaluate and adjust your information security program in light of the results of the testing and monitoring
- Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control
- Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body

Federal Trade Commission and Cybersecurity Data Security

The FTC has a Web Site devoted to helping companies protect sensitive personal and company information - https://www.ftc.gov/business-guidance/privacy-security/data-security

Provides pamphlets in topics such as (links provided):

- **App Developers: Start with Security**
- **Buying or selling debts? Steps for keeping data secure**
- **Careful Connections: Keeping the Internet of Things Secure**
- **Complying with FTC's Health Breach Notification Rule**
- **Consumer Reports: What Information Furnishers Need to Know**
- **Data Breach Response: A Guide for Business**
- **Digital Copier Data Security: A Guide for Businesses**
- **FTC Safeguards Rule: What Your Business Needs to Know**
- **Health Breach Notification Rule**
- **Health Breach Notification Rule: The Basics for Business**
- **Mobile Health App Developers: FTC Best Practices**
- **Protecting Personal Information: A Guide for Business**
- **Small Business Computer Security Basics**

Federal Trade Commission and Cybersecurity Digital Copier Data Security Brochure

Key Points made in the brochure (keep in mind this was done in 2010):

- Digital Copiers[1] are Computers
  - Require hard disk drives to manage incoming jobs and workloads
  - Hard drive in a digital copier stores data about the documents it copies, prints, scans, faxes or emails that can be stolen from the hard drive
- Copiers often are leased, returned, and then leased again or sold
  - Important to know how to secure data that may be retained on a copier hard drive, and what to do with a hard drive when you return a leased copier or dispose of one you own
  - Build in data security for each stage of your digital copier's life-cycle
- Before you acquire a copier:
  - Make sure it's included in your organization's information security policies and managed and maintained by your organization's IT staff
  - Employees who have expertise and responsibility for securing your computers and servers also should have responsibility for securing data stored on your digital copiers

[1]"Digital Copier" in the context of this pamphlet is what we would now call a Multi-Function Device

Federal Trade Commission and Cybersecurity Digital Copier Data Security Brochure

Key Points made in the brochure (keep in mind this was done in 2010):

- When you buy or lease a copier:
  - Evaluate your options for securing the data on the device. Most manufacturers offer data security features with their copiers, either as standard equipment or as optional add-on kits. Typically, these features involve encryption and overwriting
  - Another layer of security that can be added involves the ability to lock the hard drives using a passcode
  - Think ahead to how you will dispose of the data that accumulates on the copier over time
- When you use the copier:
  - Take advantage of all its security features. Securely overwrite the entire hard drive at least once a month
  - If your current device doesn’t have security features, think about how you will integrate the next device you lease or purchase into your information security plans
  - Plan now for how you will dispose of the copier securely
  - Your organization’s IT staff should make sure digital copiers connected to your network are securely integrated to protect against outside intrusions and attacks

Federal Trade Commission and Cybersecurity Digital Copier Data Security Brochure

Key Points made in the brochure (keep in mind this was done in 2010):

- When you finish using the copier:
  - Check with the manufacturer, dealer, or servicing company for options on securing the hard drive. The company may offer services that will remove the hard drive and return it to you, so you can keep it, dispose of it, or destroy it yourself. Others may overwrite the hard drive for you. Typically, these services involve an additional fee, though you may be able to negotiate for a lower cost if you are leasing or buying a new machine
  - One cautionary note about removing a hard drive from a digital copier on your own: hard drives in digital copiers often include required firmware that enables the device to operate. Removing and destroying the hard drive without being able to replace the firmware can render the machine inoperable, which may present problems if you lease the device. Also, hard drives aren't always easy to find, and some devices may have more than one. Generally, it is advisable to work with skilled technicians rather than to remove the hard drive on your own

Federal Trade Commission and Cybersecurity Start With Security Brochure

Security-Related "Lessons Learned" for previous FTC Cases released in Jun 2015

- Start with Security
  - Don't collect personal information you don't need
  - Hold on to information only as long as you have a legitimate business need
  - Don't use personal information when it's not necessary
- Control access to data sensibly
  - Restrict access to sensitive data
  - Limit administrative access
- Require secure passwords and authentication
  - Insist on complex and unique passwords
  - Store passwords securely
  - Guard against brute force attacks
  - Protect against authentication bypass

Federal Trade Commission and Cybersecurity Start With Security Brochure

Security-Related "Lessons Learned" for previous FTC Cases

- Store sensitive personal information securely and protect it during transmission
  - Keep sensitive information secure throughout its lifecycle
  - Use industry-tested and accepted methods
  - Ensure proper configuration
- Segment your network and monitor who's trying to get in and out
  - Segment your network
  - Monitor activity on your network
- Secure remote access to your network
  - Ensure endpoint security
  - Put sensible access limits in place
- Apply sound security practices when developing new products
  - Train your engineers in secure coding
  - Follow platform guidelines for security
  - Verify that privacy and security features work
  - Test for common vulnerabilities

Federal Trade Commission and Cybersecurity Start With Security Brochure

Security-Related "Lessons Learned" for previous FTC Cases

- Make sure your service providers implement reasonable security measures
  - Put it in writing
  - Verify compliance
- Put procedures in place to keep your security current and address vulnerabilities that may arise
  - Update and patch third-party software
  - Heed credible security warnings and move quickly to fix them
- Secure paper, physical media, and devices
  - Securely store sensitive files
  - Protect devices that process personal information
  - Keep safety standards in place when data is en route
  - Dispose of sensitive data securely

Federal Information Security Modernization Act of 2014 (FISMA)

I did another Google search on “cybersecurity laws” and this came up:

The three main cybersecurity regulations are ***the 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley Act, and the 2002 Homeland Security Act****, which included the Federal Information Security Management Act (FISMA)*

Federal Information Security Modernization Act of 2014 (FISMA)

- The Federal Information Security Modernization Act of 2014 (FISMA) was passed on December 8, 2014
- Amends the Federal Information Security Management Act of 2002 to:
  - Reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and
  - Set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems

Federal Information Security Modernization Act of 2014 (FISMA)

Main Roles:

- Provide for the use of automated tools in agencies' information security programs, including for periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents
- Require agencies to include offices of general counsel as recipients of security incident notices
- Require agencies to notify Congress of major security incidents within seven days after there is a reasonable basis to conclude that a major incident has occurred
- Direct agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General (GAO). Requires such reports to include: (1) threats and threat actors, vulnerabilities, and impacts; (2) risk assessments of affected systems before, and the status of compliance of the systems at the time of, major incidents; (3) detection, response, and remediation actions; (4) the total number of incidents; and (5) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information
- Authorize GAO to provide technical assistance to agencies and inspectors general, including by testing information security controls and procedures
- Require OMB to ensure the development of guidance for: (1) evaluating the effectiveness of information security programs and practices, and (2) determining what constitutes a major incident

Federal Information Security Modernization Act of 2014 (FISMA)

Main Roles:

- Direct FISIC (Federal Information Security Incident Center) to provide agencies with intelligence about cyber threats, vulnerabilities, and incidents for risk assessments
- Require OMB to ensure the development of guidance for: (1) evaluating the effectiveness of information security programs and practices, and (2) determining what constitutes a major incident.
- Direct OMB, during the two-year period after enactment of this Act, to include in an annual report to Congress an assessment of the adoption by agencies of continuous diagnostics technologies and other advanced security tools
- Require OMB to ensure that data breach notification policies require agencies, after discovering an unauthorized acquisition or access, to notify: (1) Congress within 30 days, and (2) affected individuals as expeditiously as practicable. Allows the Attorney General, heads of elements of the intelligence community, or the DHS Secretary to delay notice to affected individuals for purposes of law enforcement investigations, national security, or security remediation actions
- Require OMB to amend or revise OMB Circular A-130 to eliminate inefficient and wasteful reporting
- Direct the Information Security and Privacy Advisory Board to advise and provide annual reports to DHS