Table of Contents

CIPP Prep Guide: CIPP/US Concentration

Introduction to the CIPP Concentration Exam ................................................................. 6
  The CIPP Exam .............................................................................................................. 6
  CIPP/US Concentration ............................................................................................... 6
  CIPP Guide’s Prep Guide ............................................................................................. 7

Introduction to the IAPP and the CIPP/US .................................................................. 9
  The IAPP ....................................................................................................................... 9
  IAPP Official Resources ............................................................................................. 9
  Privacy Professional Expectations .............................................................................. 10

Structure of US Law ....................................................................................................... 11
  Understanding US Law ............................................................................................... 11
  Federal Reserve System .............................................................................................. 14
  Federal Reserve Board ............................................................................................... 17
  Office of the Comptroller of the Currency ................................................................. 20
  Self-Regulatory Programs ......................................................................................... 23
  Trust Marks ................................................................................................................. 26

Enforcement of US Privacy & Security Laws ............................................................... 29
  CIPP Applied – Unfair & Deceptive Trade Practices .................................................. 29
  Global Privacy Enforcement Network (GPEN) ............................................................ 31
  PCI DSS ......................................................................................................................... 33
  Summary ....................................................................................................................... 34

  CIPP Exam Preparation ............................................................................................. 35
  PCI DSS 2.0 Updates and Changes ............................................................................ 36

Information Management from a US Perspective ....................................................... 39
  Developing Privacy Programs: US Approaches ......................................................... 39
  Multi-National Corporation (MNC) Information Systems Planning ......................... 42
Information Systems & Information Resource Management ........................................45
Incident Response Programs .................................................................................48
Information Management Training ......................................................................51
Information Management: Accountability .............................................................54
E-Discovery vs. EU Data Protection: Conflict .......................................................57
E-Discovery vs. EU Data Protection: Solutions .....................................................60
End-of-Chapter Review .........................................................................................63
Cross-Sector FTC Privacy Protection ..................................................................67
Federal Trade Commission Act ............................................................................67
FTC: Privacy Enforcement Actions .......................................................................70
FTC: Security Enforcement Actions .....................................................................72
COPPA: The Children’s Online Privacy Protection Act .......................................75
Medical ..................................................................................................................79
HIPAA: Health Information Portability and Accountability Act ..........................79
HIPAA Enforcement Process .................................................................................82
CIPP Applied: HIPAA & CVS Case Study ............................................................85
Health Information Technology for Economic and Clinical Health Act (HITECH Act) ........89
CIPP Applied – The Cost of Data Breaches ............................................................92
CIPP Applied – WPF’s Medical Identity Theft Map .............................................95
Financial ...............................................................................................................97
Fair Credit Reporting Act (FCRA) ........................................................................97
Fair and Accurate Credit Transactions Act of 2003 (FACTA) ..............................101
The Gramm-Leach-Bliley Act (GLBA) .................................................................104
Red Flags Rule: Delayed Enforcement & Amendments .....................................106
Dodd-Frank Wall Street Reform and Consumer Protection Act .......................110
The Consumer Financial Protection Bureau .......................................................113
Education ..............................................................................................................115
Family Educational Rights and Privacy Act of 1974 ............................................115
Telecommunications & Marketing .....................................................................117
Telemarketing Regulations & Requirements .....................................................117
Email Privacy & CAN-SPAM Act ......................................................................120
Junk Fax Prevention Act (JFPA) ..........................................................................123
The Wireless Domain Registry ..........................................................................126
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telecommunications Act of 1996 and Consumer Proprietary Network Information</td>
<td>128</td>
</tr>
<tr>
<td>Video Privacy Protection Act of 1988</td>
<td>131</td>
</tr>
<tr>
<td>Cable Communications Privacy Act of 1984</td>
<td>134</td>
</tr>
<tr>
<td>End-of-Chapter Review</td>
<td>137</td>
</tr>
<tr>
<td>Law Enforcement &amp; Privacy</td>
<td>151</td>
</tr>
<tr>
<td>Access to Financial Data</td>
<td>151</td>
</tr>
<tr>
<td>Electronic Communications Privacy Act of 1986</td>
<td>154</td>
</tr>
<tr>
<td>Communications Assistance for Law Enforcement Act (CALEA)</td>
<td>157</td>
</tr>
<tr>
<td>National Security &amp; Privacy</td>
<td>160</td>
</tr>
<tr>
<td>Foreign Intelligence Surveillance Act of 1978</td>
<td>160</td>
</tr>
<tr>
<td>USA-PATRIOT Act</td>
<td>163</td>
</tr>
<tr>
<td>USA-PATRIOT Act Controversies</td>
<td>165</td>
</tr>
<tr>
<td>Civil Litigation &amp; Privacy</td>
<td>168</td>
</tr>
<tr>
<td>Privacy Protection Act of 1980</td>
<td>168</td>
</tr>
<tr>
<td>e-Discovery Basics</td>
<td>171</td>
</tr>
<tr>
<td>CIPP Applied – e-Discovery</td>
<td>173</td>
</tr>
<tr>
<td>End-of-Chapter Review</td>
<td>176</td>
</tr>
<tr>
<td>Introduction to Workplace Privacy</td>
<td>178</td>
</tr>
<tr>
<td>Human Resources &amp; Workplace Privacy</td>
<td>178</td>
</tr>
<tr>
<td>Workplace Privacy: Trends &amp; Developments</td>
<td>181</td>
</tr>
<tr>
<td>Workplace Privacy: Regulation at the US Department of Labor</td>
<td>184</td>
</tr>
<tr>
<td>Workplace Privacy: Equal Employment Opportunity Commission</td>
<td>187</td>
</tr>
<tr>
<td>Workplace Privacy: National Labor Relations Board</td>
<td>190</td>
</tr>
<tr>
<td>Occupational Safety and Health Act</td>
<td>194</td>
</tr>
<tr>
<td>Workplace Privacy: US Securities and Exchange Commission</td>
<td>196</td>
</tr>
<tr>
<td>Civil Rights Act of 1964</td>
<td>199</td>
</tr>
<tr>
<td>Americans with Disabilities Act</td>
<td>202</td>
</tr>
<tr>
<td>Genetic Information Nondiscrimination Act (GINA)</td>
<td>205</td>
</tr>
<tr>
<td>Privacy: Before, During &amp; After Employment</td>
<td>208</td>
</tr>
<tr>
<td>Employee Background Screening Basics</td>
<td>208</td>
</tr>
<tr>
<td>Employee Background Screening: A closer look at requirements and methods</td>
<td>212</td>
</tr>
<tr>
<td>Psychological and Personality Testing in Employment Screening</td>
<td>214</td>
</tr>
<tr>
<td>Problems with Background Screening in the Workplace</td>
<td>217</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Social Media Analytics in Employee Recruitment</td>
<td>220</td>
</tr>
<tr>
<td>Employee Monitoring &amp; Privacy Expectations</td>
<td>222</td>
</tr>
<tr>
<td>CIPP Applied – We’re not Facebook friends! Employee screening through social media sites</td>
<td>225</td>
</tr>
<tr>
<td>End-of-Chapter Review</td>
<td>228</td>
</tr>
<tr>
<td>Federal vs. State Authority</td>
<td>238</td>
</tr>
<tr>
<td>CIPP Applied – Proposed bill shows states’ rights sometimes fall to bad federal legislation</td>
<td>238</td>
</tr>
<tr>
<td>Driver’s Privacy Protection Act (DPPA)</td>
<td>241</td>
</tr>
<tr>
<td>CIPP Applied – Consumer Protection Laws: States Trump Federal</td>
<td>243</td>
</tr>
<tr>
<td>Successfully Responding to Data Breaches</td>
<td>244</td>
</tr>
<tr>
<td>CIPP Applied – NASA under Attack</td>
<td>248</td>
</tr>
<tr>
<td>Anti-Bullying Legislation in the United States: Children &amp; Cyberbullying</td>
<td>250</td>
</tr>
<tr>
<td>Anti-Bullying Legislation in the United States: Workplace Bullying</td>
<td>253</td>
</tr>
<tr>
<td>End-Of-Chapter Review</td>
<td>256</td>
</tr>
<tr>
<td>Definitions</td>
<td>259</td>
</tr>
<tr>
<td>Appendix A – The CIPP/US CBK Outline</td>
<td>262</td>
</tr>
</tbody>
</table>
Introduction

CIPP Prep Guide
CIPP/US Concentration

Introduction to the CIPP Concentration Exam

The CIPP Exam
The International Association of Privacy Professionals (IAPP) devised the Certified Information Privacy Professional (CIPP) as a means of identifying a baseline competence in the field of privacy. There are several additional specialization areas that extend the measured excellence of a professional into the Public Sector (CIPP/G), United States Privacy (CIPP/US), Canadian Privacy (CIPP/C), European Privacy (CIPP/E) and Information Technology (CIPP/IT). All flavors of the CIPP require successfully passing the Foundations exam, followed by the specialization. The IAPP split the Foundations exam into three segments. Since the Official Reference Guide was written before the September 2008 exam updates, the sectioning is not obvious. It is readily apparent in the updated CBK outline. A passing score is 70% (84 points) on the 120-item exam.

CIPP/US Concentration
The CIPP program launched in October 2004 and was the first professional certification ever to be offered in information privacy. It has quickly become the major credential in the field of privacy.

The CIPP/US concentration represents a major credential in information privacy and is the IAP"s largest educational program, with a few thousand CIPP/US-certified professionals working in the field today.

The CIPP/US credential requires a strong foundation in the US privacy environment and a thorough understanding of privacy laws and regulations, and comprehension of the legal requirements for responsible transfer of sensitive personal data to/from the US, the EU and other jurisdictions.
CIPP Guide’s Prep Guide

The IAPP suggests the following textbooks when preparing for the CIPP/US exam:

- *US Private-Sector Privacy: Law and Practice for Information Privacy Professionals*, Peter P. Swire & Kenesa Ahmad

These resources include a fair deal of reference material that most would find inaccessible without a law library. The IAPP offers a 30-question practice test as well.

Our goal is quite simple: to prepare you for the CIPP/US exam. This includes a succinct, fully referenced/hyperlinked study guide distilled to impart all the information a CIPP/US candidate needs. Our interactive flashcard and test software reinforces Prep Guide concepts, and our planned audio/video presentations serve to quickly review key privacy topics. We expect you will find our methods exemplary and see us as “Your Guide to the CIPP.”

Using the Prep Guide

Throughout the Prep Guide, you’ll notice a few icons highlighting key ideas. These topics are of particular importance, and by concentrating on these sections, the examination should seem a bit more familiar.

This concept is a no-brainer and will definitely be on the exam. Know it well, and you’ll rack up a few easy points on the exam without wasting time thinking about the answers. If you don’t get it, find a way to, either by reading the hyperlinks, asking questions on the discussion forums or good old-fashioned research.

Privacy is more than the CIPP/US exam. As a certified professional, this concept should be etched in your memory for future application on the job front.

There is a time and place for everything, and now may not be either. This icon designates a little deeper detail, explaining the more technical or historical aspects of a specific problem. Read this section, but you don’t feel you need to commit it to rote memory.
Expect trouble with this one. This icon marks easily confused concepts, stumbling blocks, or other ideas where it’s hard not to trip up.
The IAPP
The International Association of Privacy Professionals (IAPP) is a worldwide, privately held corporation organized in 2000 with the goal of advancing the state of privacy and providing a platform for sharing concerns and best practices. There are over 5,200 members worldwide.¹

IAPP Official Resources
The IAPP has several resources for candidates of the CIPP exams. The complete set of resources may be found on the IAPP web site.²

The CIPP/US Common Body of Knowledge per the IAPP
The CIPP/US CBK as of 3/6/2013 is listed in Appendix A and updates may be found online.³

Case Study Guide
The IAPP offers The IAPP Information Privacy Case Book, written by Margaret P. Eisenhauer, Esq., CIPP. This publication is the first comprehensive analysis of the current state of privacy and data security enforcement internationally. It is available from the IAPP web site for USD$65.00.

Classes
The IAPP also offers a two-day, interactive certification prep class in various cities worldwide.⁴

¹ “IAPP and GDD form Strategic Partnership.” IAPP Online. 9 July 2008. 6 March 2013. https://www.privacyassociation.org/about_iapp/media/2008_07_09_iapp_and_gdd_partnership
³ IAPP Privacy Certification: Outline for the CIPP Course and Certification. https://www.privacyassociation.org/media/pdf/certification/CertificationFoundation_2.0.0.1.pdf
Privacy Professional Expectations

The IAPP expects successful candidates to amass a wide breadth of privacy knowledge. The CIPP credential demonstrates a strong foundation in US privacy laws and regulations, as well as an understanding of the legal requirements for the responsible transfer of sensitive personal data to/from the US, the EU and other jurisdictions. Subject matter areas covered in the CIPP Exam include:

- The U.S. legal system: definitions, sources of law and sectoral model for privacy enforcement
- U.S. federal laws for protection of personal data: FCRA and FACTA, HIPAA, GLBA, COPPA and DPPA
- U.S. federal regulation of marketing practices: TSR, DNC, CAN-SPAM, TCPA and JFPA
- U.S. state data breach notification and select state laws
- Regulation of privacy in the U.S. workplace: FCRA, EPP, ADA and ECPA, plus best practices for privacy and background screening, employee testing, workplace monitoring, employee investigation and termination of employment

Note that in order to become CIPP/US certified, you must successfully complete the Certification Foundations exam, followed by the CIPP/US module exam.
Three Branches of US Government

The US federal government comprises three branches: executive, legislative and judicial. Each of their functions and structures are elaborated in the table below.

<table>
<thead>
<tr>
<th>Functions</th>
<th>Executive Branch</th>
<th>Legislative Branch</th>
<th>Judicial Branch</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enforcement of laws</td>
<td>Creation of laws</td>
<td>Interpretation of laws</td>
</tr>
<tr>
<td>Made up of</td>
<td>President</td>
<td>Congress (House &amp; Senate)</td>
<td>Federal courts</td>
</tr>
<tr>
<td></td>
<td>Vice-President</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cabinet</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Federal Agencies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checks &amp; Balances</td>
<td>President appoints Federal Judges</td>
<td>Congress confirms any presidential appointees</td>
<td>Determines if laws are constitutional</td>
</tr>
<tr>
<td></td>
<td>President is able to veto laws passed by Congress</td>
<td>Congress can override presidential vetoes</td>
<td></td>
</tr>
</tbody>
</table>
Sources of Law in the US

1. **Statutes** – local, state or federal laws that have been enacted by Congress
2. **Regulations** – published by regulatory agencies (e.g. FTC; Federal Trade Commission)
3. **Case Law** – decisions published by the court
4. **Common Law** – principles/rights of individuals that exist, though they are not covered by statutes

How to Analyze a Law

1. Why does this law exist?
2. Who is covered?
   *Does it apply to me?*
3. What is covered?
   *What are the activities the law talks about?*
4. What is required or prohibited?
   *What do I have to do?*
5. Who enforces the law?
   *What’s the risk?*
6. What happens if there is no compliance?
   *What are the penalties for non-compliance?*

Privacy Regulators in the US

- **FTC** (Federal Trade Commission) – lead agency overseeing privacy as a consumer protection issue. The FTC functions as a resource for the other agencies.
- **FCC** (Federal Communications Commission) – collaborates with the FTC on TCPA and CAN-SPAM
- **Department of Commerce** – collaborates with the FTC on Safe Harbor
- **OCC** (Office of the Comptroller of the Currency) – works with FTC on FCRA
- **HHS** (Department of Health & Human Services) – oversees HIPAA
- **OCR** (Office of Civil Rights)
- **CMS** (Center for Medicare & Medicaid Services)
- **DOT** (Department of Transportation)
- **State Attorneys General** – responsible for enforcement of privacy legislation
CIPP/US Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Branches of government (I.A.a.)
- Sources of law (I.A.b.)
- Regulatory authorities (I.A.d.)
**Federal Reserve System**

The **Federal Reserve System** (the Fed) is the central bank of the United States. It was created by the Congress to provide the USA with a “safer, more flexible, and more stable monetary and financial system.” It is an independent entity within the government. However, it remains subject to oversight by the Congress, which often reviews its activities and can alter its responsibilities by statute.

**History**

The **Federal Reserve Act** was initially enacted in 1913. The Fed comprises of the Board of Governors in Washington and twelve Federal Reserve Banks situated throughout the country.

The Federal Reserve was enacted due to the failure of the national banks to provide effective funding which led to an increased likelihood of financial panics. A severe crisis in 1907 led to Congress establishing the **National Monetary Commission**, which made proposals to create an institution that would prevent such financial disruptions.

**Federal Open Market Committee**

The **Federal Open Market Committee** (FOMC) is a body established by the Federal Reserve Act to govern the system’s operations in the market for US government securities and certain other instruments. It is the principal source on US national monetary policy. The committee is comprised of twelve voting members, including all seven board members, the president of the Federal Reserve Bank of New York, and four of the eleven other Reserve Bank presidents, who serve in rotation.

In addition, the Directors of each Reserve Bank contribute to monetary policy by making recommendations about the appropriate discount rate, which are subject to final approval by the Governors.

**Role of the Federal Reserve System**

The Fed’s duties broadly fall into four general areas:

- Conducting the nation’s monetary policy by influencing the monetary and credit conditions in the economy in pursuit of maximum employment, stable prices, and moderate long-term interest rates (known as the Fed’s dual mandate).
- Supervising and regulating banking institutions to ensure the safety and soundness of the nation’s banking and financial system and to protect the credit rights of consumers.
- Maintaining the stability of the financial system and containing systematic risk that may arise in financial markets.
- Providing financial services to depository institutions, the US government, and foreign official institutions, including playing a major role in operating the nation's payments system.

The Federal Reserve Act states that the Board of Governors and the Federal Open Market Committee (FOMC) should seek “to promote effectively the goals of maximum employment, stable prices, and moderate long-term interest rates.”

**Consumer Protection**

In regard to consumer protection, the Federal Reserve’s responsibilities include:

- Writing and interpreting regulations to carry out many of the major consumer protection laws.
- Reviewing bank compliance with the regulations.
- Investigating complaints from the public about state member banks’ compliance with consumer protection laws.
- Addressing issues of state and federal jurisdiction.
- Testifying before Congress on consumer protection issues.
- Conducting community development activities.

**International Role**

The activities of the Federal Reserve and the international economy influence each other. Therefore, when deciding on the appropriate monetary policy for achieving basic economic goals, the Board of Governors and the FOMC consider the record of US international transactions, movements in foreign exchange rates, and other international economic developments.

**Supervisory Role**

The Federal Reserve shares supervisory and regulatory responsibilities for domestic banking institutions with the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation (FDIC), and the OTS.

The primary supervisor of a domestic banking institution is generally determined by the type of institution that it is and the governmental authority that granted it permission to commence business. Banks that are chartered by a state government are referred to as state banks; banks that are chartered by the OCC are referred to as national banks.
Funding

As an independent entity within government the Fed does not receive any funding from Congress. The income of the Fed is primarily from the interest on U.S. government securities that it trades through open market operations. Other sources of income include interest on foreign currency investments, fees received for services, and interest on loans to depository institutions.

After paying its expenses, the Federal Reserve transfers any surplus earnings over to the US Treasury.

Summary

This article provides a brief overview of the Federal Reserve System, which represents the central bank of the United States. The Federal Reserve was enacted due to the failure of the national banks to provide effective funding which led to an increased likelihood of financial panics. The article takes a look at the roles and responsibilities of the Federal Reserve.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Federal Reserve Board (I.A.d.v.1.)
Federal Reserve Board

The Federal Reserve Board of Governors is the main governing body of the Federal Reserve System. The board comprises of a chairman and six members. The current chairman of the Board is Ben Bernanke, whose role as chairman is scheduled to last until January 2014.

Appointment

The President of the United States has the power to appoint members of the Board of Government. Any such appointment must be carried out with the consent of the Senate. The board members are elected for 14-year terms, with the chairman and vice-chairman of the Board each elected for four-year terms. The appointments are staggered so that one term expires on January 31 of each even-numbered year. Although the Senate must consent to any appointments to the board, they have no further role in the Fed’s policies. However, the Fed must “work within the framework of the overall objectives of economic and financial policy established by the government.” On this basis, the Federal Reserve describes itself as “independent within the government.”

Role and Responsibilities of the Federal Reserve Board

The Board also plays a major role in the supervision and regulation of the US banking system. It has supervisory responsibilities for state-chartered banks that are members of the Federal Reserve System, bank holding companies, the foreign activities of member banks, the US activities of foreign banks, and Edge Act and agreement corporations (limited-purpose institutions that engage in a foreign banking business). The Board and, under delegated authority, the Federal Reserve Banks, supervise approximately 900 state member banks and 5,000 bank holding companies.

The Board’s responsibilities required thorough analysis of domestic and international financial and economic developments. The Board carries out those responsibilities in conjunction with other components of the Federal Reserve System. The Board also supervises and regulates the operations of the Federal Reserve Banks, exercises broad responsibility in the nation’s payment system, and administers most of the nation’s laws regarding consumer credit protection.

Some regulations issued by the Board apply to the entire banking industry, whereas others apply only to member banks. The Board also issues regulations to carry out major federal laws governing consumer credit protection, such as the Truth in Lending, Equal Credit Opportunity, and Home Mortgage Disclosure Acts. Many of these regulations apply to various lenders outside of the banking industry as well as to banks.
Policy regarding open market operations is established by the Federal Open Market Committee (FOMC). However, the Board of Governors has sole authority over changes in reserve requirements, and it must approve any change in the discount rate initiated by a Federal Reserve Bank.

**Publications**

The Board publishes detailed statistics and other information about the Federal Reserve System’s activities and the economy in publications such as the quarterly *Federal Reserve Bulletin*, the monthly *Statistics Supplement*, and separate statistical releases.

**Chairman of the Board**

The Chairman of the Board has a number of other duties, such as occasional meetings with the President of the United States and regular meetings with the Secretary of the Treasury. The Chairman also has formal responsibilities in the international arena. For example, he is the alternate US member of the board of governors of the IMF. He is also a member of US delegations to key international meetings, such as the *Group of Seven (G7)* meetings.

As required by the Federal Reserve Act, the Chairman of the Board of Governors testifies before the Senate Committee on Banking, Housing and Urban Affairs and the House Committee on Financial Services on or about February 20 and July 20 of each year. The Chairman’s testimony addresses the efforts, activities, objectives, and plans of the Board of Governors and the FOMC with respect to the conduct of monetary policy, as well as economic development in the US and the prospects for the future. Concurrently, the Board of Governors must submit a report on these same issues to the House and Senate committees before which the Chairman testifies.

**Auditing**

The Board is audited annually by a major public accounting firm. In addition, the *Government Accountability Office* (GAO) generally exercises its authority to conduct a number of reviews each year to look at specific aspects of the Federal Reserve’s activities. The audit report of the public accounting firm and a complete list of the GAO reviews are available in the Board’s *Annual Report*, which is sent to Congress during the second quarter of each calendar year. Monetary policy is exempt from audit by the GAO because it is monitored directly by Congress through written reports, including the semi-annual *Monetary Policy Report to the Congress*, prepared by the Board of Governors.
Summary

This article looks at the Federal Reserve Board of Governors, the main governing body of the Federal Reserve System. As a major player in the supervision and regulation of the US banking system, the Federal Reserve Board takes on several roles and responsibilities, which are explored in this article.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Banking regulators – Federal Reserve Board (I.A.d.v.1.)
Office of the Comptroller of the Currency

The Comptroller of the Currency is the administrator of national banks and chief officer of the Office of the Comptroller of the Currency (OCC). The OCC supervises more than 2,000 national banks and federal savings associations and about 50 federal branches and agencies of foreign banks in the USA. The Comptroller is also a director of the Federal Deposit Insurance Corporation (FDIC) and NeighborWorks® America.

Appointment

The Comptroller of the currency is a presidential appointment that is subject to Senate advice and consent. The Comptroller is appointed for a five-year term. The current Comptroller is Thomas J. Curry who was sworn in on April 9, 2012.

History

The Office of the Comptroller of the Currency was created as a bureau of the US Department of the Treasury in 1863. Its duty was to organise and administer a system of nationally chartered banks and create a uniform national currency. In 1864, the National Bank Act substantially altered the original bill, expanding upon the basic frameworks already in place and clarifying many of the provisions.

The original short-term purpose of the Act was to raise cash to finance the Civil War. Prospective national bank organisers were required to purchase interest-bearing US government bonds in an amount equal to one-third of their paid-in capital. In the long-term, the purchased bonds were to be deposited with the Treasury and held as security for a new national currency. It was believed that a national currency would assist in creating a sense of nationalism among the citizens at that time.

The Federal Reserve Act of 1913 altered the role of the OCC. It was no longer required to administer the US monetary system, and its duties became primarily an organisation of “national bank examiners charged with ... maintaining the safety and soundness of the banks they supervised.” The OCC played a major role in the US reaction to the Great Depression by reviewing banks and deciding which banks could be re-issued with banking licenses.
Current Role

The OCC’s current mission is to “charter, regulate, and supervise all national banks and federal savings associations.” They also “supervise the federal branches and agencies of foreign banks.”

The OCC acquired some of the functions of the Office of Thrift Supervision in July 2011 (along with the Federal Reserve Board and the Federal Deposit Insurance Corporation). The OTS was established in 1989 and was the primary regulator of Federal Savings Associations (or Federal thrifts). The OTS was also supervised Savings and Loan Holding Companies (SLHCs) and some state-chartered institutions. The OCC now has the power to regulate federal thrifts.

Duties of the OCC

In regulating national banks and federal thrifts, the OCC has the power to:

- Examine the national banks and federal thrifts.
- Approve or deny applications for new charters, branches, capital, or other changes in corporate or banking structure.
- Take supervisory action against national banks and federal thrifts that do not comply with laws and regulations or that otherwise engage in unsound practices. Remove officers and directors, negotiate agreements to change banking practices, and issue cease and desist orders as well as civil money penalties.
- Issue rules and regulations, legal interpretations, and corporate decisions governing investments, lending, and other practices.

The OCC’s activities are based on four objectives that support the agency’s mission to ensure a stable and competitive national system of banks and savings associations:

- Ensure the safety and soundness of the national system of banks and savings associations.
- Foster competitions by allowing banks to offer new products and services.
- Improve the efficiency and effectiveness of OCC supervision, including reducing regulatory burden.
- Ensure fair and equal access to financial services for all Americans.

Funding

The OCC does not receive any funding from Congress but is primarily funded by assessments on national banks and federal savings associations. National banks and federal thrifts pay for their examinations and for any processing of corporate applications. The OCC also receives revenue from its investment income.
Summary

The Comptroller of the Currency is the administrator of national banks and chief officer of the Office of the Comptroller of the Currency (OCC). The article provides an overview of the history of the OCC as well as its current roles and responsibilities as a banking regulator in the US.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Comptroller of the Currency (I.A.d.v.2.)
Self-Regulatory Programs

The emergence of e-commerce in the late 20th century has allowed for the creation of a continually expanding online marketplace. However, the ease with which online companies can collect information from their customers has raised concerns about consumer privacy. The advantage of self-regulation as a means of addressing this issue is considered to be that it provides the necessary flexibility to address evolving online business models.

**Online Behavioral Advertising (OBA)** involves the tracking of consumers’ online activities in order to deliver personal advertising. This practice allows business to specifically target their advertisements towards individual customers. The data collected is generally not personal identity information, but data relating to their browsing history. The below principles have been drafted from a number of sources and are intended as a means of applying consumer-friendly standards to OBA.

**Principles**

The [Federal Trade Commission](https://www.ftc.gov) (FTC) published their “Self-regulatory principles for online behavioral advertisements.” Their principles are:

1. **Transparency and Consumer Control**

   Every website where data is collected should provide a clear, concise, consumer-friendly, and prominent statement that (i) data about consumers’ activities online is being collected for use in providing advertisements about products and services tailored to individual consumers’ interests, and (ii) consumers can choose whether or not to have their information collected for such purposes.

   Furthermore, where the data collection occurs outside the traditional website context, the FTC recommends that companies “develop alternative measures of disclosure and consumer choices that meet the standards required.”

   The Better Business Bureau (BBB) recommends that compliance with this principle will result in new links and disclosures on the web page or advertisement where online behavioral advertising occurs. It will offer consumers the ability to exercise choice regarding the collection and use of data for online behavioral advertising.

   The BBB Transparency and Consumer Control Principles also have provision for Service Providers (ISPs). These provide that ISPs must provide additional notice regarding the online behavioral advertising that occurs by use of their services, obtain the consent of users before engaging in online behavioral advertising, and take steps to de-identify the data used for such purposes.
ii) **Reasonable security, and limited data retention, for consumer data**

Companies should provide reasonable data security measures so that behavioral data does not fall into the wrong hands, and should retain data only as long as necessary for legitimate business or law enforcement needs. The FTC states that "the protections should be based on the sensitivity of the data [and] the nature of a company’s business operations, the types of risks a company faces, and the reasonable protections available to a company."

iii) **Affirmative express consent for material changes to existing privacy promises**

Before a company uses previously collected behavioral data in a manner that is materially different from promises made when the company collected the data, it should obtain affirmative express consent from the consumer.

The FTC states that this principle is limited to retroactive changes. Therefore it would not include prospective changes, such as where a company may change its privacy policy and then collect and use new data under the new policy.

iv) **Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising**

Although the FTC did not provide any definition of 'sensitive data', they stated that the most prominent examples included financial data, data about children, health information, precise geographical location information, and Social Security numbers.

The BBB stated that the heightened protection for children’s data should be taken into consideration along with the protective measures contained in the Children’s Online Privacy Protection Act 1998.

Further to these principles, the BBB considered a number of further principles to be advantageous in promoting self-regulation.

v) **Educate consumers and businesses about online behavioral advertising**

The National Telecommunications & Information Administration (NTIA) states that "public education is essential to assessing and shaping attitudes. When people can be presented with rationale for the collection of such data, and the safeguard provided, an appropriate balance between collection and privacy can be struck."

vi) **Entities involved in OBA advertising should be accountable and should implement policy programmed to further adhere to these principles.**

The BBB calls for programs to have mechanisms by which they can police entities engaged in online behavioral advertising and help bring these entities into compliance. Programs will also publicly report instances of uncorrected violations.
Conclusion

The above principles are the most widely accepted relating to self-regulation. At the outset, it was stated that self-regulation provided businesses with the flexibility to apply regulations. However, it is debatable whether privacy self-regulation is ever likely to fully succeed in its goals. Without legislation or regulation to make companies accountable, how can customers be assured that their data is secure? At present, the FTC has no effective means of statutory regulations due to limits on its authority. However, the sheer size of the internet makes it unlikely that sufficiently secure regulations can ever be fully applied and advances in technology could mean that regulations would become obsolete almost as soon as they are published.

Summary

This article takes a look at common principles that relate to self-regulation. The article explores how self-regulation offers the advantage of providing the necessary flexibility to address evolving online business models. The article also briefly explores the FTC’s “Self-regulatory principles for online behavioral advertisements.”

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Self-regulatory programs and trust marks (I.A.d.vii.)
**Trust Marks**

In theory, there are no major differences between traditional and electronic commerce. However, the additional complexity of conducting business online (e.g. expertise in internet browsing and obtaining knowledge about the retailer website) requires a higher level of trust on the part of the consumer than traditional shopping methods. Despite advances in technology, the fear of scammers remains more prevalent for internet shoppers and can result in a reluctance to engage in online transactions.

**Origins**

A trust mark is considered to be a symbol or sign that represents an assurance of some understood message i.e. a seal of approval. It is often displayed on the homepage of a website with the permission of a trusted third party in order to prove that the online shop complies with a voluntary code of conduct to provide the best possible online business environment for the consumer. Because of the rise of internet fraud during the early years of e-commerce, the online industry had to provide a suitable response to these problems.

Websites were encouraged to be independently authenticated and audited. This was the beginning of the online trust marks and they were originally logo marks such as Visa or McAfee.

**Importance of Trust Marks**

It is suggested that the trust marks are most crucial when the customer is reaching a decision on what and where to buy (pre-contractual stage). The online retailer has to attract the customer at this point and trust marks can make the information provided appear more reliable.

During the contractual stage, trust marks remain important as it is still possible for the user to change their mind before entering into the binding contract. Trust marks may also encourage the customer to provide the required personal and payment details in situations where they may otherwise have doubts about the security of the system.

The importance of trust marks can be indicated by a 2009 Harris Interactive survey which found that more than 90 % of people expressed concerns when shopping on new or unknown sites. Almost half of the surveyed customers terminated orders because of security fears. The survey also suggested that 47 % of customers will look for trust marks to ensure security when shopping on a lesser known site.
Obtaining a Trust Mark

An online retailer gains a trust mark by submitting a satisfactory self-assessment report referring to the business's security, privacy and practices.

Online trust marks can be broken into four types, depending on the assurance being given:

- **Personal Privacy** – These symbols indicate that a site protects user information and rights.
- **Business Reputation** Services such as BBBOnline (BBB - Better Business Bureau) requires businesses to have a physical presence, be in business for at least one year, and have a positive track record of handling complaints.
- **Secure Transactions** – Companies such as PayPal have increased the ease at which online retailers can arrange payments in a secure, trustworthy, manner. Ensuring security for payments is a fundamental task for online vendors.
- **Security and Vulnerability Scanning** – Malicious content planted on websites and misconfigured websites can allow hackers and scammers to access customer details. Regularly scheduled vulnerability scanning can identify and correct these flaws promptly.

Verisign have noted a number of reasons why having individual trust marks are valuable to online retailers.

- **Level of Display** – The more sites that use the trust mark, the more likely it is that customers will trust the mark and therefore the website. The reputation of the mark will obviously depend on the websites that the marker allows to display their logo.
- **Exposure Breeds Familiarity** – If customers are viewing the trust mark on sites that they are familiar with an associate value begins to exist between the customer and the trust mark.
- **Recognition** – The public perception of the trade mark is fundamental to the level of trust that the customers will have with it.

**Examples**

BBBOnline award two types of seals. The first, Reliability Seal, is awarded to companies that have been business for at least one year and possess a ‘satisfactory complaint handling record with the BBB’. The second is the Privacy Seal. It is awarded to businesses that subscribe to responsible information practices such as clearly advertising and implementing online privacy policies conforming to the BBBOnline required principles of disclosure, choice, and security.

A Verisign seal communicates that “the website and its owner or operator have been authenticated by Verisign, and that the website uses SSL and/or another service to enhance security.”
Conclusion

Trust marks remain an important factor in creating a positive impression on online customers and representing a certain level of consumer confidence in vendors. Consumers continue to look for some level of security when shopping online and will not purchase from websites that they do not consider to be trustworthy. With the level of online competition available to vendors, having the right trust marks may be sufficient to encourage customers to complete their transactions.

Summary

This article takes a look at trust marks, be a symbol or sign that represents an assurance of some understood message (i.e. a seal of approval), which are an essential component in ecommerce. There are four major types of trust marks: 1) Personal privacy; 2) Business reputation; 3) Secure transactions; 4) Security and vulnerability scanning. The article also provides two examples of popular trust marks.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Self-regulatory programs and trust marks (I.A.d.vii.)
**CIPP Applied – Unfair & Deceptive Trade Practices**

In the United States, we’re dependent on the overlapping and sometimes confusing patchwork of legislation and regulations because the US employs a **sectoral** versus **comprehensive** approach to privacy. This legal patchwork sometimes includes state laws in addition to federal, which most see as simply another hurdle towards doing business in that state. In some cases, related but more stringent laws in the state were already passed. In those situations only minor modifications are needed for state compliance with a newly signed federal statute.

The Federal Trade Commission (FTC) and state Attorneys General enforce federal and state laws of consumer privacy protection for **Unfair or Deceptive Trade Practices** (UDTP).

One recent example was the **state of Maine's consumer protections, which are more restrictive than the federal laws** with respect to cigarette labeling. The state brought suit against a tobacco manufacturer for violating the state’s deceptive trade law, which the manufacturer argued was out of line due to the federal Cigarette Labeling Act. The **Supreme Court decision upheld the State’s right to pass more restrictive legislation**, pointing out:

"Neither the Labeling Act's pre-emption provision nor the Federal Trade Commission’s actions in this field pre-empt respondents' state law fraud claim. Pp. 5–20.

(a) **Congress may indicate pre-emptive intent** through a statute’s express language or through its structure and purpose. See *Jones v. Rath Packing Co.*, 430 U. S. 519, 525. When the text of an express pre-emption clause is susceptible of more than one plausible reading, courts ordinarily “accept the reading that disfavors pre-emption.”

The rationale in (a) requires express language for a federal law to negate a state’s right to create more restrictive legislation. The first citing by the high court becomes the **contentious issue for House Bill H.R. 2221**, proposed by Illinois Representative Bobby Rush. The bill tackles several tough interstate commerce issues, placing the FTC in charge of disposal regulations for **obsolete or abandoned paper records containing personal information**, notifications and verification requirements for information brokers. Section 6 of the so-called **Data Accountability and Trust Act** includes a provision reading:

(a) …This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State, with respect to those entities covered by the regulations issued pursuant to this Act, that expressly--
1. requires information security practices and treatment of data in electronic form containing personal information similar to any of those required under section 2; and
2. requires notification to individuals of a breach of security resulting in unauthorized acquisition of data in electronic form containing personal information.

(b) Additional Preemption-

1. IN GENERAL- No person other than the Attorney General of a State may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.

This would strike several of the state privacy and notification laws (possibly including California’s SB 1386), stripping the State’s rights and growing Washington’s power. It also bars the state Attorneys General from bringing suit, possibly in an effort to avoid a double jeopardy situation. There are numerous case studies of the FTC and state Attorneys General working hand-in-hand for consumer protection; why this law tries to hamstring the situation is a bit of a mystery.

One more interesting note on Representative Rush’s proposal – the bill also places an encryption exemption on breach notification. As we noted in another article on corporate disposal policies, hackers and researchers seem to notice protection missteps and use them to bypass security provisions just like encryption.

“The encryption of data in electronic form shall establish a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data. Any such presumption may be rebutted by facts demonstrating that the encryption has been or is reasonably likely to be compromised.”

The law has a ten year lifespan, which should be a decent requirement before the Advanced Encryption Standard (AES), currently the de-facto encryption standard (and as yet to be compromised), ages beyond its effectiveness.

President Obama’s May 20th, 2009 Memorandum on the Subject of Preemption and state’s rights quotes Justice Brandeis saying, “[i]t is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.”

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Regulatory authorities – Federal Trade Commission (I.A.d.i.)
- Regulatory authorities – state Attorneys General (I.A.d.vi.)
- Unfair and deceptive trade practices (I.B.d.)
Global Privacy Enforcement Network (GPEN)

In June 2007, members of the OECD adopted a Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. This Recommendation required member countries to foster the establishment of an informal network of Privacy Enforcement Authorities (PEAs). This network of authorities would be responsible for the following activities:

- Discuss practical aspects of privacy law enforcement cooperation
- Share best practices in addressing cross-border challenges
- Work to develop shared enforcement priorities
- Support joint enforcement initiatives and awareness campaigns

Forming the Network

In October 2010, thirteen PEAs came together to form the Global Privacy Enforcement Network (GPEN) to aid cross-border cooperation. These countries included: Canada, US, France, New Zealand, Israel, Italy, Australia, Ireland, Spain, the UK, the Netherlands and Germany. The GPEN is responsible for enforcing laws and investigations to protect personal data and encourages its members to develop shared enforcement policies and support joint enforcement initiatives.

Upon announcement of the new network, Marie Shroff, New Zealand Privacy Commissioner commented,

“The challenges in obtaining redress for consumers whose privacy has been compromised in today’s digital environment can be daunting. GPEN is part of a collective effort to provide more effective cross-border enforcement and complaints resolution. This is as relevant for a small economy in the South Pacific as it is for Europe and North America. And New Zealand is pleased to play its part.”

Mission & Committee

According to its statement of mission:

GPEN connects privacy enforcement authorities from around the world to promote and support cooperation in cross-border enforcement of laws protecting privacy.

It primarily seeks to promote cooperation by:

- Exchanging information about relevant issues, trends and experiences;
- Encouraging training opportunities and sharing of enforcement know-how, expertise and good practice;
- Promoting dialogue with organizations having a role in privacy enforcement;
Creating, maintaining and supporting processes or mechanisms useful to bilateral or multilateral cooperation; and
Undertaking or supporting specific activities

The GPEN Committee is made up of a four to five person committee to perform the following tasks:

- Process applications from authorities wishing to participate in GPEN and make recommendations for membership to participating authorities.
- Activate user accounts for access to GPEN website.
- Edit public pages of website.
- Facilitate arrangements from GPEN teleconferences and meetings.
- Liaise with OECD Secretariat over administration of website.

In general, the GPEN Committee performs functions that support the network’s mission.

Summary

This article introduces the Global Privacy Enforcement Network (GPEN), an international group of privacy enforcement officials who have come together to aid information sharing efforts and provide international support of global privacy issues. The GPEN was established in 2010, as a result of an OECD recommendation published in 2007.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Cross-border enforcement issues – GPEN (I.B.g.)
PCI DSS

Retail e-commerce sales are amounting in the tens of billions of dollars in the United States alone. However, in 2006, credit card fraud was the most common form of identity theft, accounting for 25% of all reported identity thefts in the US. This meant that over $50 billion was lost to credit card fraud in that year alone.

Credit Card Fraud in Context

The following high-profile cases of credit card fraud underscore the need for security practices, such as the PCI DSS:

- February 2005: Bank of America loses 1.2 million customer records, although there was no evidence that the records had come into the wrong hands.
- June 2005: Merchant payment-processing provider, CardSystems, is sued for failing to provide adequate protections for the personal information of over 40 million customers.
- February 2006: Approximately 400,000 debit card accounts were disclosed by retail merchants.
- January 2007: A MoneyGram (a payment service provider) server was unlawfully accessed, revealing the names, addresses, phone numbers and bank account numbers of some 79,000 customers.
- January 2007: The credit/debit card numbers of over 45 million customers was stolen from the TJX IT system.

What is PCI DSS?

In 2004, American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International created the Payment Card Industry (PCI) data security framework. Before developing this standard, each company had a proprietary set of information security requirements, which presented a challenge to participants in multiple brand networks. The uniform set of information security requirements they developed became known as the PCI Data Security Standard (PCI DSS), which applies to all payment channels: retail, mail orders, phone orders and e-commerce.

PCI DSS is comprised of twelve security requirements (aka the “digital dozen”), which are as follows:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update anti-virus software/programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for employees and contractors.

**Compliance with PCI DSS**
Compliance with PCI DSS is becoming more and more important for businesses of all sizes. Demonstrating compliance with the standard proves to customers that an organization has secure systems that can be trusted with their sensitive payment card information. As a result, customers are more likely to build trust in the brand, become repeat customers and recommend the business to others. Compliance with PCI DSS can also develop a business' reputation with acquirers and payment brands. It can also make other compliance processes easier (e.g. with HIPAA, SOX, etc.).

There are three main stages of compliance:
1. **Collecting and Storing** – This involves the secure collection and tamper-proof storage of log data so that it is available for analysis.
2. **Reporting** – This is the ability to prove compliance should an audit arise. The organization should also show evidence that data protection controls are in place.
3. **Monitoring and Alerting** – This involves implementing systems to enable administrators to monitor access and usage of data. There should also be evidence that log data is being collected and stored.

**Non-Compliance**
There are numerous negative consequences of non-compliance with the PCI DSS. Compromised payment card data has negative outcomes for consumers, merchants and financial institutions. Compromised data can damage an organization's brand reputation. Breaches of account data can result in loss of sales, relationships, diminished community standing and decreased share prices, for publicly traded companies.

Other negative consequences of non-compliance may also include:
- Lawsuits
- Cancelled accounts
- Payment card issuer fines (which could amount up to $500,000 per incident)
- Government fines
- Insurance claims
- Loss of ability to process payment card transactions

**Summary**
This article explores the PCI DSS (Payment Card Industry Data Security Standard), developed in 2004 by a number of stakeholders in the payment card industry. The PCI DSS is comprised of twelve security requirements, which are referred to as the “digital dozen.” The article discusses the advantages of compliance, as well as the necessary stages to achieve compliance with the PCI DSS.
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Self-regulatory enforcement (I.B.h.)
PCI DSS 2.0 Updates and Changes

The Payment Card Industry (PCI) recently made adjustments to their Data Security Standards (DSS) 2.0 guidelines. These modifications came into effect at the end of June 2012, impacting the security of customer card information and network design. This article takes a look at the essentials of the changes.

Another look at the PCI-DSS 2.0

The PCI DSS released version 2.0, the most recent version of the standard, in October 2010. The vast majority of the changes in this version of the standard are quite minor. The most significant change in this version is the requirement for assessed entities to have the appropriate procedures and documentation in place to demonstrate where cardholder data is (and is not) located.

Previously, most PCI assessments reviewed the known cardholder data flows. While providing as much detail as possible about known cardholder data flows is essential, the PCI Council is asking for something more. Companies are actually required to do something in order to demonstrate where there is no cardholder data. Simply understanding where cardholder data should be is not sufficient; now, companies need to demonstrate that they know where it could not be.

Framework for Cardholder Data Discovery

Cardholder data flows and ecosystems differ quite a bit from company to company. However, the generic cardholder data discovery methodology outlined below provides a common starting point for many companies.

- Identify in-scope entities and determine if there is any cardholder data present. In-scope entities refer to any systems, applications, databases and people who have access to cardholder data.
There are a number of ways to collect the information needed. This may include:

- **Reviewing data flow diagrams.** This is similar to the activities described in PCI DSS version 1.2. The information uncovered through this process can then be used to determine which individuals should be considered “in-scope,” and then move forward into additional information gathering.

- **Interviews.** Once known cardholder data flows have been documented, interviews should be conducted with people who use the cardholder data; administer the cardholder data; or who have administrative access to cardholder data. Interviews are an excellent way to determine if scope can be reduced if the cardholder data is not really necessary. Often, it’s the people who use the cardholder data that are able to assist the most in finding out where it is actually stored.

- **Penetration testing.** Some companies use penetration testing in order to demonstrate that there are no covert channels, application weaknesses, network architectural flaws, or other means, to show that this sensitive data is protected appropriately.

- **Forensics analysis.** This can help define the scope by carrying out close assessment. Some companies do this to show that there is no logical means of cardholder data inadvertently spilling over to a system, application or log file.

### What do the changes mean?

**According to Alex Quitter,** director of PCI at Qualys, “This is an evolution of the requirements. You need to show a process for risk rankings.” What it means is obtaining information about known vulnerabilities from publicly-available sources, whether this is vendor security alerts or elsewhere. From there, risks should be prioritized to the organization’s network as they relate to protecting PCI data. Risks should be prioritized as high, medium or low.

The modifications to the standard place an added emphasis on vulnerability risk rating, which means that the PCI DSS rule is far more stringent in terms of language regarding scanning requirements. It now requires organizations to show proof of passing an internal vulnerability assessment.

Such assessments must be completed on a quarterly basis, and after any significant changes in the company. They must be performed by a qualified party. They must also show a “passing result,” which means that any high vulnerabilities to internal networks must be resolved.

### Summary

This article takes a look at recent changes to the Payment Card Industry Data Security Standards (PCI-DSS) version 2.0. The changes affect risk rankings, vulnerabilities and demonstrating cardholder data flows. This article outlines the changes and also offers a methodology for cardholder data discovery.
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Self-regulatory enforcement (I.B.h.)
Information Management from a US Perspective

Developing Privacy Programs: US Approaches

Guided by privacy legislation and internal privacy policies, US federal government agencies and departments strive to protect citizens’ personal information and privacy rights. This article introduces the privacy practices of three federal departments: the US Census Bureau, the Internal Revenue Service (IRS) and the US Department of Defense.

US Census Bureau: Data Stewardship

The Census Bureau’s objective is to produce accurate, relevant statistics on US economy and population. It is legally and ethically obligated to protect the privacy and confidentiality of the individuals who offer their data. According to the Bureau’s mission statement, “We honor privacy, protect confidentiality, share our expertise globally, and conduct our work openly.” One of the Bureau’s strategic goals is to “Foster an environment that supports innovation, reduces respondent burden, and ensures individual privacy.” The approach that the Census Bureau takes to maintain the trust of US citizens is referred to as “Data Stewardship.”

Data stewardship is the formal process by which the Bureau remains responsible and accountable for data protection throughout the data lifecycle. This refers to the time which someone responds to a survey, all the way to the release of statistical data products. Each survey and program under the Census Bureau’s responsibility is required to comply with data stewardship policies at every step in the process.

There are three ways that the Bureau protects personal information:

1) **Federal Law** – Federal law protects personal information. Title 13 of the US Code protects the confidentiality of all information provided to the Bureau. Violation of Title 13 results in severe penalties.

2) **Privacy Principles** – In addition to federal legislation, the Bureau has developed its own set of privacy principles, which are guidelines for all its activities. Privacy principles include the Bureau’s responsibilities to protect personal information, as well as individuals’ rights as survey respondents.

3) **Statistics Safeguards** – These include methods to ensure that statistics released by the Bureau do not identify individuals or businesses. All data products are extensively reviewed and analyzed. Disclosure avoidance methodologies (e.g. data suppression, data modification) are also applied.
IRS: Privacy Office

Like other federal agencies, the IRS is committed to protecting Americans’ privacy rights. It notes that individuals’ privacy rights are protected by the following:

- Internal Revenue Code
- Privacy Act of 1974
- Freedom of Information Act
- IRS policies and practices

In addition to adhering to the above, the IRS also has a Privacy Office, which ensures that personal information entrusted with the IRS is protected appropriately. The Office addresses questions regarding IRS privacy policies and concerns regarding how the IRS uses and collects personal information.

Department of Defense: Privacy Policy

The Department of Defense (DoD) provides a website as a public service by the Office of the Assistant Secretary of Defense – Public Affairs. Like other websites, there are options for individuals to offer the DoD personal information and the DoD is responsible for treating this information appropriately. The DoD maintains a wide variety of physical, electronic and procedural safeguards to protect personal information from unauthorized disclosure or data breach.

According to the DoD’s website Privacy Act Statement:

“If you choose to provide us with personal information… we will only use that information to respond to your message or request. We will only share the information you give us with another government agency if your inquiry relates to that agency, or as otherwise required by law. We never create individual profiles or give it to any private organizations. Defense.gov never collects information for commercial marketing.”

Summary

This article takes a look at approaches to privacy protection at various agencies of the US federal government: the US Census Bureau, the Internal Revenue Service (IRS) and the US Department of Defense (DoD). Each department or agency is guided by federal privacy legislation, as well as internal policies and practices.
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Privacy program development – US perspective (I.C.b.)
Multi-National Corporation (MNC) Information Systems Planning

An information system is a set of people, data, and procedures that work together to provide useful information. It is essential to the functioning of a complex multi-national corporation (MNC). The need for an effective Management Information System (MIS) function is particularly crucial for the survival and success of MNCs. Because of their international structure, MNCs are vulnerable to the uncertainties associated with the multiple political, cultural, and economic systems within which they operate.

An organisation’s MIS is a system for obtaining, processing, and delivering information that can be used in managing the organisation in order to improve the performance of the organisation through the implementation of Information Technology (IT). Modern technology allows organisations access to information regardless of the physical distance between the source and the use of the information. The newfound MIS capability not only allows more timely decision making, it also enables better control of foreign subsidiaries or operations.

Strategies to Create Global Information Systems

Akmanligil and Palvia provide the following primary strategies for developing a Global Information System:

i) Development with a multinational design team

The participation of personnel from multiple sites can help create a plan the meets the requirements of all regions and can also increase the likelihood of mutual acceptance of the software and adhering to international standards.

ii) Parallel Development

By this process the construction of the various subsystems are performed at the local sites and integrated. The various systems are coordinated via common development methodologies via shared software tool and e-mail.

iii) Central Development

In this process the system is developed at the headquarters and then installed at the subsidiaries. The advantages of the process are lower costs, certainty of a standard operating procedure, and better communication. However the disadvantages may include resistance by subsidiaries or incompatibility with the requirements of some regions.
iv) Core vs. Local Development

This process relies on a centralised system that develops a common global solution while taking into consideration and accommodating the regional needs of the subsidiary. This process can allow the subsidiary to alter the centralised approach to suit their separate requirements. This process can minimise local conflicts and also increase coordination.

v) Best In-Firm Software Adoption

The process involves selecting the best software currently in use within the organisation and implementing it throughout the group. However, this process may require some modifications due to the differences in technological resources. In such instances, it may be beneficial to provide a region with its own modified version of the required software. Such a process can increase maintenance costs.

vi) Outsourced Custom Development

Outsourcing provides that the system is developed by an external company. Outsourcing can be used to implement and enforce global standards along with reducing costs. The disadvantages to this process may be that management lose a certain amount of control and may also lose a competitive advantage.

vii) Unmodified Package Software Acquisition

By this process the organisation simply purchase the required software instead of developing it themselves. With such unmodified packages, agreements can be made with vendors to provide better support and ensure that future modifications will be compatible. The disadvantages may be that the standard packages may not completely meet the requirements of the firm and modification may be necessary.

viii) Modified Package Software Acquisition

By this process the software required is modified by the vendors prior to acquisition. In many cases, only minimal modification is recommended due to the high costs of development and maintenance that can be incurred.

ix) Joint Development with Vendors

This process involves the hiring of vendors to create and help administrate the system in its entirety. This process can have the advantages of ensuring that the latest technology is available and can allow be implemented quickly.
Conclusion

Choosing the best process is not a foolproof plan but some of the items that should be taken into consideration include the characteristics of the organisation, the requirements of the system, the differences between the headquarters and the subsidiaries, and the standards and skills of the staff. Choosing the correct process is essential to the success of any IS project. However, its success is not solely based on the successful implementation of one of the above processes, but may also be based on the quality of the information, satisfaction of the user and the impact that the system may have on the organisation.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Other key considerations for US-based MNCs (I.C.i.)
Information Systems & Information Resource Management

With the increasing globalisation of business, multinational corporations (MNCs) are no longer able to compete in the format of having nationally independent subsidiaries. Instead, the need has arisen for MNCs to integrate their subsidiary activities across geographical divisions. However, building an efficient international information system to support information exchange and parent-subsidiary linkage involves the resolution of many technical and managerial Information Systems (IS) issues, stemming from both the parent MNC and its subsidiary.

Parent Organisation Issues

The problems associated with the planning and control of a multinational Information Resource Management function (IRM) have led to difficulties as MNCs attempt to deal with the complexities that geographical and associate differences have imposed on their international IRM functions.

The Management Information System’s (MIS) role in the IRM planning and coordination process is to provide the assistance required to implement such plans along with providing strong coordination. The corporate MIS planning role includes developing, maintaining, and enhancing the plan procedures and processes, along with identifying key issues and conducting studies to assess the technology.

Subsidiary Company Issues

Lai’s survey indicated that the top three IS issues rated by foreign affiliates of MNCs include:

i) IT infrastructure
ii) Information architecture
iii) Communication networks

Subsidiaries of MNCs generally operate in less developed countries may have issues and restrictions such as inefficient communication networks and IT infrastructures. Such technological restrictions can have many detrimental effects on the subsidiaries, including curtailing the ability to make IS strategic decisions, increasing IS costs due to inefficient handling of IT resources, causing high error rates during data transmission, creating difficulties for system maintenance, and increasing the complexity of technology transfer and integration. If these technology infrastructure issues are unresolved, foreign subsidiaries would not be able to take advantage of economies of scale and the cost efficiencies associated with the technological advances in IT. Thus, subsidiaries need to build a responsive information infrastructure to support and enhance their existing and future applications.
When information infrastructure and IT architecture are not solidly implemented, the subsidiary’s
data and resources will be scattered throughout their computing networks without a structured
plan, making the distribution process and data integration impossible.

**Information Resource Management Planning**

Some of the key changes to evolve traditional IRM planning into a viable and dynamic process
include the following:

i) The inclusion of additional levels of individuals, organisations, and functional groups
must be involved in the planning process through more participative multi-level and
multi-process mechanisms.

ii) Strong business and IRM plan links must be established by joint business and IRM
coordination and planning at all levels involving multiple executive, functional and
IRM personnel across business and geographic regions.

iii) Development of a uniform and coordinated IRM planning language, process,
structure, and cycle.

iv) The perception of what IRM contributes to the business must change. Understanding
the business and related IRM strategic postures can help provide the best possible
plan for the future.

v) The role of the corporate IRM staff should be well defined and limited to only those
activities where its expertise is either clearly recognised, through creditability, or
established by corporate policy. Utilise corporate IRM personnel, both generalists
and specialists, as catalysts and change agents to question, motivate, encourage,
and guide the business units on a multi-level basis.

vi) Recognise that the IRM concept requires a macro approach to managing a growing
and vital asset that will involve significant changes in awareness, structure,
discipline, and political loyalties. The conceptual architecture of the IRM environment
must be established.

vii) Separation of IRM responsibilities between strategic direction and day-to-day
operational support is a critical prerequisite for success. Adequate resources must
be allocated to this process.

viii) Operations must start to develop systems by using their chart of accounts to track
the true course of information processing in every segment of the business. This will
establish a more accurate baseline to evaluate the benefits of IRM in the future.

ix) Focus on proactive, positive, incremental, and iterative strategies that propel the IRM
Committee into the new role of the strategic integrators of the organisation’s
information resources through the support of a multi-disciplinary IRM staff function.
Information Resource Management Functions

To plan effectively for the IRM functions, the following six planning phases should be completed for all IRM components. Each phase includes a series of activities:

i) **Environmental Reference Base** – This provides an external and internal environmental profile, both domestically and internationally, of the factors influencing existing business and IRM conditions in terms of problems, stages of penetration, resource levels, strengths etc.

ii) **Issues and Opportunities** – This identifies and relates business issues and objectives with IRM issues, opportunities, goals and objectives from a corporate, domestic, and international perspective.

iii) **Strategic Analysis of Alternatives** – This evaluates the various available strategic IRM alternatives in terms of organisation structures, mission statements, benefits, strategies, risks, obstacles, vulnerabilities, resource requirements, key assumptions, and contingency plans.

iv) **Strategic Objective Setting and Commitment** – This involves the actual planning and development of strategies along with the IRM implementation strategy.

v) **Systems Development Methodology** – This attempts to convert the strategic IRM plan into separate work projects through a systems development methodology, which consists of multiple phases, management approvals, and resource allocations.

vi) **Follow-up and Measurement** – This involves a review mechanism of the plan based on a series of pre-established requisites such as budgetary reviews, capital expenditure linkages to the plan, major project checkpoint reviews, periodic performance audits, adherence to standards and/or guidelines, and other monitoring mechanisms.

Summary

This article explores technical and managerial Information Systems (IS) issues experienced by multi-national corporations (MNCs). The article lists key concepts in today’s information resource management planning, as well as six planning phases involved in information resource management.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Key considerations for US-based multi-national corporation (I.C.i.)
Incident Response Programs

Research shows that consumers have widespread distrust of many organisations business practices, including how they collect, use and retain personal information. A security incident refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such an event.

According to CERT, a security incident can have the following definitions:

i) Violation of an explicit or implied security policy
ii) Attempts to gain unauthorised access
iii) Unwanted denial of resources
iv) Unauthorised use of electronic resources
v) Modification without the owner’s knowledge, instruction, or consent
vi) Theft of displaced property

An Incident Response Program (IRP) is a plan created to provide a defined, organised and coordinated approach for handling any potential threat to computers and data. One of the means of creating a good incident response plan is the establishment of a Computer Security Incident Response Team (CSIRT).

Computer Security Incident Response Team

A CSIRT is established to provide a quick and effective response to computer related incidents such as virus infections, improper disclosure of confidential information to others, service interruptions, breach of personal information, computer hacking, and other events that could compromise computer security. The CSIRT’s purpose is to prevent a serious loss of profits and retain public confidence, reputation, or information assets by providing an immediate and effective response to any unexpected events involving computer information systems, networks or databases.

CSIRT staff should be responsible for the following areas:

- Development and preservation of the program and the document
- Defining and classifying incidents
- Determining the tools and technology utilised in intrusion detection
- Determining if incident should be investigated and the scope of such an investigation (i.e. law enforcement agencies, forensic work)
- Securing the network
- Conducting follow-up reviews
- Promoting awareness throughout the organisation.
Creating a Successful Information Response Program

For an IRP to be successful, the maintenance of the program be updated to reflect any organisational / infrastructure changes and newly discovered vulnerabilities.

Due to the nature and amount of business being done through the Internet, minimising security vulnerabilities and responding to security incidents in an efficient and thorough manner can become critical to business continuity.

Gartner supplies an estimate of figures for the cost of an IRP. They estimate that a large organisation and / or an organisation largely dependent on e-commerce should budget for the following:

- Two dedicated CSIRT employees reporting to the chief information security officer
- $251,000 per-person start-up capital expenditure
  - Hardware - $144,000
  - Software - $80,000
  - Education - $27,000 per year
  - Stand-alone CSIRT command central reporting center
  - Telecommunications – 24 telephone lines (8 each for voice, data, fax)
  - External services – investigations and forensics - $100,00 per year

Implementing an Incident Response Program

Reporting/Discovery

- It is important that an organisation ensures that their information systems are kept properly updated. The Internet can provide a valuable resource that allows organisation to monitor the release of any upgrades from vendors.
- CSIRT Members should be alerted an any high-risk security incidents automatically
- A database should be developed to track all reported security incidents.
- All reported incidents should be classified in a high/medium/low risk range to facilitate the appropriate actions to take.

Response

CSIRT employees should be made responsible for performing the initial investigation to determine if an incident has occurred. Some of the solutions that can prevent intrusions include blocking the IP from which the attack is being generated, disabling the affected user ID, removing/blocking the system from the network and/or shutting the system down.
Investigation

Depending on the level of intrusion, an organisation may decide to perform a forensic investigation that can allow the affected organisation to gain a better understanding of the intrusion and the attacker. By performing such an investigation, the organisation may be able to obtain information on the existing security vulnerabilities in the organisation’s systems, any changes to be made to the systems and/or applications, identification of the sources of the attack, and methods of information disclosure, including acts of espionage.

Recovery

Recovery includes ensuring that the attacker’s points of penetration and any associated vulnerabilities have been eliminated and all systems have been restored.

Follow-up

Perhaps the most important follow-up to an incident is ensuring that the organisation has learned from the incident, in order to reduce the likelihood of such incidents re-occurring.

Summary

This article takes a look at incident response programs (IRPs), plans created to provide a defined, organised and coordinated approach for handling any potential threat to computers and data. It outlines the stages involved in creating an IRP: reporting/discovery, response, investigation, recovery and follow-up.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Information management from a US perspective – training (I.C.d.)
Information Management Training

Training Program

The following is a basic framework for a training program in Information Management.

**Information Security**

To ensure that security is strong within an organisation, employee training should include the following:

- Being made aware of their responsibilities in regard to information security.
- Trained to make decisions on the protection and classification required for information.
- Trained to understand how to deal with sensitive material.
- Trained to be aware of the appropriate methods of communication and destruction of sensitive material.
- Trained to understand the importance of being required to remove or change the level of protection or classification of information.

**Information Management**

- Being made aware that they are responsible for managing information within the organisation.
- Trained that effective information management ensures that information is available, protected and disposed of in accordance with company policy and legislative requirements.
- Trained to delete transitory records i.e. information sources that are only required for a limited period of time or to complete a routine action.

Good quality information management will yield the following rewards:

- Quality information is created and provided.
- Organisation programs and services are efficient.
- Decisions are documented and the information is available for future use.
- Information is protected in accordance with company policy and legislative requirements.
- Information is disposed of in accordance with company policy and legislative requirements.

**E-mail**

Employees should be trained in the following with respect to dealing with their e-mails.

- Being made aware of their responsibilities with respect to e-mail.
- Being made aware that email messages can be part of official company records and what messages are transitory and should therefore be disposed of.
- Trained to recognise when an e-mail should be saved.
- Trained to understand what type of e-mails should be saved.
- Trained to be familiar with Information Management email best practices. Such practices include using meaningful and descriptive titles on email attachments to ensure accuracy in filing/classifying the message.

**Privacy and Personal Information**

Personal information is considered to be high risk information and should be dealt with accordingly. Employees should be trained in the following with respect to privacy and personal information:

- Trained in the general guidelines required for the collection of personal information.
- Being made aware of their responsibilities with respect to the protection and management of personal information.
- Being made aware of relevant policy or legislation that directly related to privacy and personal information.

**Training for Information Management in MNCs**

It is important for organisations to ensure that their training plan on information management remains current, as it is easy for training plans to become out-of-date or invalid. Typically, training is based on retrospective behaviour and situations and may not be sufficient to direct the desired actions. In order to overcome such problems, managers are trained via socialisation practices that guide and indoctrinate members to work as the organisation requires. Such approaches are considered to be effective means of controlling the behaviours of organisational members and are central to the notion of manager’s management.

Martinez and Jarillo note that “Socialisation is an informal and subtle mechanism that can be added to the structural and formal mechanisms to help MNCs cope with their complex environments.” They further state that “Socialisation practices incorporate two control mechanisms: corporate acculturation and the transfer of parent company nationals to foreign subsidiaries. Both rely on corporate culture as a means of control, although in different ways.”

**Training for the Incident Response Manager**

The Incident Response Manager is responsible for implementing the incident response policy and procedures. This individual should work with management to ensure all users are trained in their response role. Continuous awareness training and monitoring are important for strong computer security. Response drills are good tools to test the plan.
Training for Accountability

All staff should receive training in Information Management accountability. The role of the Information Management is to support these staff by ensuring that the appropriate training and support is available. Highly specialised service providers that handle more sensitive data, such as health and financial data, may require particularly thorough awareness training.

Training for Data Handlers

All individuals with responsibilities that include data handling should be properly trained in the procedures and best-practices used to protect information. This should include one-on-one training on IT security and data stewardship.

Summary

This article outlines a basic framework for an information management training program.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Information management training from a US perspective – training (I.C.d.)
Information Management: Accountability

The concept of accountability can be used to describe a wide array of phenomena. Within organisations, accountability can describe attitudes, behaviours, and mechanisms at various levels within the organisation.

A definition proposed by Hall et al states:

“Accountability refers to a real or perceived likelihood that the actions, decision, or behaviours of an individual, group, or organisation will be evaluated by some salient audience, and that there exists the potential for the individual, group, or organisation to receive either rewards or sanctions based on this expected evaluation.”

Information privacy and security are interrelated information management responsibilities and disciplines. They both need to be optimised and are most successful when their respective planning systems are integrated.

In relation to customer privacy, accountability would be considered to be the acceptance of responsibility for personal information protection. An accountable organisation must have appropriate policies and procedures in place that promote good practices that constitute a privacy management program.

Accountability in the context of outsourcing

Verified security and privacy practices have the potential to enhance the brand of a product. In an increasingly competitive market, companies will leverage trusted information management to attract and keep customers who have entrusted their personal data to them. Assuring that service providers responsibly use and safeguard personal data is becoming an increasing factor in outsourcing.

One of the most important factors in creating a strong information management system in the context of outsourcing includes the ability and willingness of service operators to demonstrate commitment and competence to operate within an accountability framework that requires them to meet obligations that originate from multiple industries, companies and national systems.

It is difficult to govern cross-border data flows under any one country’s laws or legal frameworks. Attempting to apply potentially conflicting privacy obligations from various countries can impede the sharing of information and consequently interrupt business operations and communications.

A practical and effective business accountability framework will encourage privacy and information management provisions to be explicit in sourcing contracts. Clear contractual requirements will communicate data protection responsibilities of clients that are relayed to service providers. It is suggested that following the below factors will ensure that sourcing contracts reflect the required accountability:
The outsourcing contracts must reflect the obligations that incur alongside the data being outsourced.

These contracts may be drafted in order to reflect any legal obligations emanating from the originating country for the particular data. The contracts may also be drafted to include privacy promises made to a consumer by the organisation that collected the personal data for a particular purpose but may also be shared with a service provider.

The obligations that come with the data being shared should reflect the details of the information being shared, rather than generic references to applicable laws. This may require clients to better identify the data being shared with service providers, its sources and the obligations attendant to the data, including limitations on use.

**Accountability Framework**

It is important to document and communicate what the accountability structure is for information management. As such, organisations will want to ensure their accountability structure includes:

- Clear accountability statements for the management of information within the organisation.
- A mechanism for coordinating information management within the organisation and to ensure that information management is integrated within the organisation.
- Clear identification and education around roles and responsibilities in specific business contexts.

Although accountability should extend to all sections of an organisation, it is important for organisations to develop a formal model of information management to provide leadership, expertise, and a focal point for the management of information assets. A means of achieving this model would be to create an official role to overlook the establishment of this model, best described as the Information Director, who is accountable for:

- Supporting other managers in identifying and meeting information management needs.
- Developing information management plans for the organisation
- Leading and monitoring progress in implementing the Information Management Framework within the organisation
- Facilitating a coordinated approach to information management in the organisation to ensure all sectors of the organisation are working on the same targets.
- Developing information management policies, standards and guidelines related to collection, creation, storage, access, retention, and disposal of information.
Summary

This article takes a look at accountability in information management, or the acceptance of responsibility for personal information protection. An accountable organisation must have appropriate policies and procedures in place that promote good practices that constitute a privacy management program.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Information management – accountability (I.C.e.)
E-Discovery vs. EU Data Protection: Conflict

**USA**

Electronic Discovery (or e-Discovery) is the process of identifying, preserving, collecting, preparing, reviewing, and producing electrically stored information (ESI) in the event of a legal request for such information. Rule 34 of the Federal Rules of Civil Procedure 2006 provide that a party may serve on any other party a request for any ESI within any medium, or ‘any designated tangible things.’ The scope of pre-trial discovery in the US is considered to be the widest of any common law country.

Some of the most common areas of US litigation where data may be affected include:
- Document preservation in anticipation of proceedings before US courts or in response to requests for litigation;
- Pre-trial discovery requests in US civil litigation;
- Document production for US criminal and regulatory investigations;
- Criminal offences in the US relating to data destruction.

US companies must pre-emptively retain all documents that may be relevant to actual or reasonably foreseeable litigation. Where a company fails to preserve such information, they may be fined or possibly be subjected to criminal sanctions.

Thus far, US courts have not been lenient to parties raising EU privacy concerns. This places US companies in the difficult position of having to decide whether to breach EU data protection laws or US e-discovery court orders.

**EU**

In the EU, data protection is protected by Article 8 of the Charter of Fundamental Rights of the European Union. It is primarily regulated by the Data Protection Directive 95/46/EC, which considers personal data to be “any information that relates to an identified or identifiable natural person.” Although this directive has been implemented throughout the EU, the level of protection is uneven. For this reason, the European Commission has proposed a new Data Protection regulation that is intended to apply the same principles of protection throughout the EU States.

Directive 95/46/EC contains two primary principles relating to discovery obligations:

i) Purpose Limitation

This limitation provides that European companies should only collect personal data for specific, legitimate purposes, and should use, disclose and retain the data only as needed for those purposes. Using business records which contain personal data in the course of litigation is a secondary use of the data which, generally, is not permitted.
ii) Export limitation

Article 25 of the directive provides that the transfer of personal data to a third country may only take place if the third country ensures an ‘adequate’ level of protection. The US is not currently on the list of countries that are considered to provide such protection.

Article 26 of the directive provides exceptions to this restriction for cases such as where the data transfer is legally required in legal disputes. This exception has been interpreted strictly and is considered to be inapplicable to e-discovery requests except where individual EU member states have enacted exceptions.

Many civil law countries in the EU do not have any formal discovery processes. France and Spain, for example, restrict disclosure to documents that are admissible at trial. In Germany, litigants are not required to disclose documents to the other party; parties need only produce the documents that will support their case.

Conflict

There is a conflict for US firms that contain affiliates in EU countries. On the one hand, federal and state rules authorise the retention and production of all relevant data, even if the data is located outside of the US. However, EU data protection laws lay down strict rules for personal data, which severely restricts the transfer of data to jurisdictions outside of the EU.

Until the EU publish further regulations, it is unlikely that any such issues will be resolved and US companies will need to ensure that their discovery policies comply with the strictest EU data protection laws.

The Article 29 Working Party of the EU stated that there is a need to reconcile the requirements of the US litigation rules and EU data protection provisions. The Working Party report provided three relevant grounds that may allow the processing of personal data to be legitimate:

- Where there is consent from the data subject;
- Where the compliance with the pre-trial discovery requirements is necessary for compliance with a legal obligation;
- Where the compliance with the pre-trial discovery requirements is necessary for the purposes of a legitimate interest. This basis would only be acceptable where such legitimate interests are not “overridden by the interests for fundamental rights and freedoms of the data subject.”

Conclusion

Conflict remains between US and EU data laws. This conflict is starting to be recognised on both sides of the Atlantic. However, at present, no definitive solution exists.
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Resolving multinational compliance conflicts (I.C.j.)
E-Discovery vs. EU Data Protection: Solutions

The conflict between US e-discovery and EU data protection means that many multinational companies have to choose between restricting an e-discovery or acting in breach of data protection legislation. This article considers the possible solutions available for multinational companies.

Co-ordination

It is important that companies that are subject to a legal action are familiar with the legal position in other jurisdictions if required. This may be achieved by co-ordination between legal counsels and the sharing of information with their counterparts and the relevant courts on the requirements of European data protection law. Although US courts have become more understanding of the challenges posed by European data protection laws, it is still advantageous to ensure that the court is aware of a company’s individual requirements.

Understanding

Before entering into discussion with the opposition counsel, companies should carry out an internal assessment of its own situation in order to create an understanding of how its data processing works, the type of data involved, and where and how long it is stored. The company should also establish the possible scope of an e-discovery order so that it can be aware of any potential issues relating to specific jurisdictions. The company should also have an awareness of the sensitivity of the different categories of data to assess the level of restrictions on the relevant categories.

Particular Multinational Issues

A company should be aware of the manner and locations that its processes are operating in. Many groups of companies may now have virtual employees located across the world communicating with headquarters via internet communications. This trend is making e-discovery much more complex. Many companies are off-shoring and outsourcing their processes and this has impacted data access and monitoring issues. Therefore records of these processes should also be documented for e-discovery purposes.

IT Issues

IT data management can vary from country to country depending on the technology available. Many companies, however, tend to centralise their data storage, especially with the advances in cloud computing. This means that US-based employees of multinationals often have access to data stored outside of the jurisdiction. Because of the implications of this access, companies should ensure data access across borders is properly managed and documented.
E-discovery Analysis

A firm needs to determine the data that is required to be produced in the context of an e-discovery order in order to be able to obtain the relevant documents. The firm should assess the nature of the data to see whether it is sensitive data relating to employees, customers, or third party individuals. They should assess whether the disclosure will affect company secrets or confidentiality agreements made with third parties.

The firm should also find out where the anticipated US trial will be held and according to what rules, as rules and standards may vary from state to state.

The firm should establish what legal frameworks should be complied with while conducting an e-discovery outside of the US. This includes a consideration of EU data protection legislation or ‘blocking statutes’ from local jurisdictions. The company should consider who within the company should be tasked with meeting these requirements and whether it would be beneficial to create an internal e-discovery organisation.

Compromising

A form of an acceptable compromise would be the targeted collection of data with notification provided to the affected employees, followed by a detailed questionnaire for employees to indicate the data sources that they use along with notifying the company of potentially relevant data. This enables the company to identify data easier and comply with transparency provisions under data protection legislation. Companies should also ensure that any content provided should remove the names of the employees included in the content.

Consolidation

Many multinationals are beginning to consolidate European data in one jurisdiction in order to streamline any possible e-discovery, as the rules of only one country will have to be applied. For example, Switzerland does not have any formal requirements for a guarantee of adequate data protection so long as the guarantee is adequate.

Protection of data after e-discovery

A company’s duty to protect personal data continues after the data has been transferred to the US. The standard protection procedure is for the US court to issue a protective order. This ensures that business secrets are not disclosed by anybody involved in the proceedings and ensures that the court keeps all records under seal.
Conclusion

The methods described above can assist multinational companies to comply with data protection legislation in Europe (and elsewhere). However, by adopting internal procedures to deal with e-discovery without the need of a particular legal matter, the knowledge and experience may be built up over time to deal with such matters, thus reducing the cost and burden of any future e-discovery.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Resolving multinational compliance conflicts (I.C.j.)
End-of-Chapter Review

Three Branches of US Government

<table>
<thead>
<tr>
<th>Executive Branch</th>
<th>Legislative Branch</th>
<th>Judicial Branch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functions</td>
<td>Enforcement of laws</td>
<td>Creation of laws</td>
</tr>
<tr>
<td>Made up of</td>
<td>• President</td>
<td>Congress (House &amp; Senate)</td>
</tr>
<tr>
<td></td>
<td>• Vice-President</td>
<td>Congress confirms any presidential appointees</td>
</tr>
<tr>
<td></td>
<td>• Cabinet</td>
<td>Congress can override presidential vetoes</td>
</tr>
<tr>
<td></td>
<td>• Federal Agencies</td>
<td></td>
</tr>
<tr>
<td>Checks &amp; Balances</td>
<td>• President appoints Federal Judges</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• President is able to veto laws passed by Congress</td>
<td></td>
</tr>
</tbody>
</table>

Sources of Law in the US

1. Statutes – local, state or federal laws that have been enacted by Congress
2. Regulations – published by regulatory agencies (e.g. FTC; Federal Trade Commission)
3. Case Law – decisions published by the court
4. Common Law – principles/rights of individuals that exist, though they are not covered by statutes

How to Analyze a Law

1. Why does this law exist?
2. Who is covered?
   Does it apply to me?
3. What is covered?
   What are the activities the law talks about?
4. What is required or prohibited?
   What do I have to do?
5. Who enforces the law?
   What’s the risk?
6. What happens if there is no compliance?
   What are the penalties for non-compliance?
Privacy Regulators in the US

- FTC (Federal Trade Commission)
- FCC (Federal Communications Commission)
- Department of Commerce
- OCC (Office of the Comptroller of the Currency)
- HHS (Department of Health & Human Services)
- OCR (Office of Civil Rights)
- CMS (Center for Medicare & Medicaid Services)
- DOT (Department of Transportation)
- State Attorneys General

Federal Reserve System

- US central bank
- Duties:
  1. Conduct national monetary policy
  2. Supervise and regulate banking institutions
  3. Maintain stability of financial system, contain systematic risk
  4. Provide financial services to depository institutions, US government, foreign official institutions
- Federal Reserve Act (1913)

Federal Reserve Board

- Main governing body of Federal Reserve System
- Main supervisor and regulator of US banking system

Office of the Comptroller of the Currency

- Administration of national banks
- Bureau of US Department of the Treasury
Self-Regulatory Programs

- FTC’s self-regulatory principles for online behavioral advertisements (OBA):
  - Transparency and consumer control
  - Reasonable security and limited data retention for consumer data
  - Affirmative express consent for material changes to existing privacy promises
  - Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising
  - Educate consumers and businesses about OBA
  - Entities involved in OBA should be accountable and should implement policy programmed to further adhere to these principles

- Trust mark
  - A symbol or sign that represents an assurance of some understood message (i.e. seal of approval).
  - Main types:
    - Personal privacy
    - Business reputation
    - Secure transactions
    - Security and vulnerability scanning

Unfair & Deceptive Trade Practices (UDTP)

- Enforced by FTC and state attorneys general

PCI DSS

- Uniform set of information security requirements for credit card industry
- Comprised of the “digital dozen”
- Three stages of compliance:
  1. Collecting and storing
  2. Reporting
  3. Monitoring and alerting

MNC Information Systems Planning

- Creating global information systems:
  - Development with multinational design team
  - Parallel development
  - Central development
  - Core vs. local development
- Best-in-firm software adoption
- Outsourced custom development
- Unmodified package software acquisition
- Modified package software acquisition
- Joint development with vendors

- Planning phases when creating information resource management programs:
  - Environmental reference base
  - Issues and opportunities
  - Strategic analysis of alternatives
  - Strategic objective setting and commitment
  - Systems development methodology
  - Follow-up and measurement

Incident Response Programs (IRP)

- IRP = a plan created to provide a defined, organized, coordinated approach for handling potential threats to computers and data.
- IRP stages:
  - Reporting/discovery
  - Response
  - Investigation
  - Recovery
  - Follow-up
- Security incident = adverse event in an information system and/or network, or the threat of the occurrence of such an event.

Information Management Training

- Information security
- Information management
- Email
- Privacy and personal information
- Tailored training: MNCs, incident response managers, accountability, data handlers
- Accountability framework: clear accountability statements and mechanism for coordinating info management
Federal Trade Commission Act

The Federal Trade Commission Act was passed by the US Congress in 1914 and resulted in the creation of the Federal Trade Commission (FTC), a federal agency that was tasked with the duty of investigating businesses for evidence of unfair business practices such as unfair competition or deceptive practices.

Before the FTC Act

The FTC Act is known as an ‘antitrust’ form of legislation. In the 19th and early 20th century giant corporations referred to as ‘trusts’ controlled many of the natural and basic resources of the US, such as railroads and oil, coal and gas resource. These trusts had almost total power in their respective industries and, due to the absence of competition, were able to control the market and therefore the prices which were charged.

In 1890 Congress passed the Sherman Act. This legislation made it illegal for competitors to make agreements with each other that would limit competition. The US Supreme Court cases of Standard Oil v US and American Tobacco v US held that the Sherman Act also made it illegal for a business to be a monopoly if that company is not competing fairly. The justification for this was that the Act “limited the freedom of contract by some to protect the contractual freedom of others.”

The Sherman Act resulted in the breakup of many of these huge trust organisations. However, to bypass the law many of the resulting competing companies merged to create a single conglomerate with similar control to the disbanded trusts. For example, the American Tobacco Company was a merger of 250 separate companies. To stop this practice, the Clayton Act was passed in 1914. This Act provided that such mergers were illegal if the result was that the resultant company would stifle competition.
Federal Trade Commission Act

Under the Act, the FTC was created to have five members. These members are appointed by the US President for seven-year terms.

Section 5 of the FTC

The most important section of the legislation in relation to enforcement is Section 5, which in 1914 stated that it proscribes unfair competition, and authorises the FTC to issue order prohibiting ‘unfair methods of competition.’ In 1938, the Wheeler-Lea Act expanded the authority of the FTC under Section 5 to include ‘unfair or deceptive acts or practices.’ Under Section 8 of the Act, the FTC Board has the authority to take appropriate action when unfair or deceptive acts or practices are discovered.

An act or practice is deemed to be unfair in the following circumstances:

- The act or practice must cause or be likely to cause substantial injury to consumers;
- The consumers must not reasonably be able to avoid the injury;
- The injury must not be outweighed by other benefits to consumers or to corporate competition;
- Public policy must be considered.

Whether a particular act or practice is considered to be unfair or deceptive will depend on the FTC’s analysis of the facts and circumstances of the case. Complaints received by the FTC may initially suggest that the violations were isolated incidents. However, investigations that consider that complaints, when considered in the context of additional information, including other violations or complaints, may raise concerns about unfair or deceptive acts or practices.

Conclusion

The FTC has expanded from the initial tasks set out by the Federal Trade Commission Act. For example, the FTC is also tasked with enforcing the provisions of the Children’s Online Privacy Protection Act 1998. However, much of the 1914 provisions have remained intact. The Commission is still authorised to issue orders in order prohibit unfair methods of competition. Also, the agency continues to combine formal investigation and prosecution powers with the informal authority to educate and work with companies in order to facilitate compliance with the law. The 1914 Act contained the foresight to ensure that the agency could adapt to changing conditions and shape its broad mandate to the needs of those times.
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Federal Trade Commission Act (II.A.a.)
FTC: Privacy Enforcement Actions

In its 2012 Report, the Federal Trade Commission (FTC) noted that it had brought numerous cases against companies for violating the FTC Act by making deceptive claims about the privacy and security protections they afford to consumer data, and also cases relating to the protection of children’s privacy under the Children’s Online Privacy Protection Act 1998. The FTC is also a privacy enforcement authority in the Asia-Pacific Economic Co-operation (APEC) Cross-Border Privacy Rules system that was approved by the US in 2012 and is intended to enhance the protection of consumer data moving between countries that are members of APEC. Below are a number of recent and high profile enforcement actions taken by the FTC.

Google

The FTC charged Google with deceiving customers by taking previously private information (Gmail frequent contacts lists) and making them public in order to generate custom for their new social network, Google Buzz. This was done without consent and in contravention of Google’s privacy promises. The FTC ordered that, if Google changes a product or service in a way that makes any data collected from or about consumes more widely available to third parties, it must seek affirmative express consent to such a change. In addition, the order required Google to implement a comprehensive privacy program and obtain independent privacy audits every other year for the next two decades. In a later enforcement action, the FTC claimed that Google made misrepresentations to users of the Safari internet browser that it would not place tracking ‘cookies’ or serve targeted ads to those users, violating the earlier agreement with the FTC. Because of the previous violations by Google, punitive damages were claimed by the FTC and Google reached an agreement to pay $22.5 million.

Facebook

The FTC case against Facebook included a charge that certain changes made to the website had led to information designated as being private being released in the public domain. The complaint also charged that Facebook made inaccurate and misleading disclosures relating to how much information about users’ were accessible by third party applications operating on their website. The FTC investigation discovered that most third-party applications were able to view nearly all of the users’ information, regardless of whether or not the information was necessary for the app to operate. The Commission further charged Facebook for failing to keep certain promises in relation to privacy. For example, the company informed users that it would not share information with advertisers, but it did. The company had also stated that it would make inaccessible the photos and videos of users who had deleted their accounts, and then it did not. As part of the action, the Commission ordered Facebook to obtain users’ express consent before sharing their information in a manner exceeding their privacy setting. The order also required Facebook to create and implement a comprehensive privacy program, along with
being obliged to undergo outside privacy audits for two decades following the action. Facebook were also ordered to not provide access to a user’s information once that information is deleted.

**Epic Marketing**

In their action against online advertising company Epic Marketing, the FTC claimed that the company used ‘history sniffing’ to secretly and illegally obtain sensitive medical and financial data from customers. ‘History sniffing’ is a technology that allows online operators to see what sites consumers have visited in the past i.e. their browsing history. The marketing company then used the information to send consumers targeted advertisements, despite claiming in its privacy policy that it would only collect information about consumers’ visits to sites in its network. Epic Marketing agreed to a settlement where they would delete and destroy all data collected using this process. The order also barred Epic Marketing from misrepresentations about the extent to which they maintain the privacy of data from or about a particular consumer.

**Summary**

This article reviews enforcement actions carried out by the FTC (Federal Trade Commission). High profile cases include the Google Buzz case, Facebook’s inaccurate and misleading claims, and Epic Marketing’s “history sniffing.”

**CIPP Exam Preparation**

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- FTC privacy enforcement actions (II.A.b.)
FTC: Security Enforcement Actions

Section 5(a) of the Federal Trade Commission (FTC) Act prohibits “unfair or deceptive acts or practices in or affecting interstate commerce.” The following article summarises a number of high-profile and recent enforcement actions taken by the FTC to enforce the security policies implemented under the Act.

Twitter

The FTC alleged that lapses in Twitter’s data security system allowed hackers to obtain unauthorised administrative control of twitter, giving them the capacity to view private information and send fake messages from accounts, including from the account of Barack Obama. The hackers gained access to the system by repeatedly attempting to enter a password for a site administrator. The FTC alleged that the following reasonable steps should have been taken by Twitter to prevent such hacking to occur:

- Require employees to use more difficult passwords that were not used for any other websites or networks;
- Prohibit employees from storing their passwords in plain text in their e-mail accounts;
- Suspend or disable administrative passwords after a certain number of login attempts;
- Provide an administrative login page for authorised persons rather than a general login page for site administrators and users;
- Enforce a requirement to regularly change administrative passwords;
- Restrict access to administrative controls to those staff whose roles require such access;
- Impose other restrictions on administrative access such as IP restrictions.

Under the settlement, Twitter were barred for 20 years for misleading consumers on the extent of its security protection, and were ordered to create and implement a security system that would be assessed by independent auditors for one decade following the order.

RockYou

In an action under the FTC Act and the Children’s Online Privacy Protection Act, the FTC took an action against the social media gaming company RockYou. The FTC alleged that RockYou had failed to use appropriate security measures to protect consumers’ private data, resulting in hackers gaining access to users’ e-mail addresses and RockYou passwords. The FTC also charged RockYou with allowing almost 200,000 children under 13 to access the site without providing notice or obtaining the parental consent as required under COPPA. RockYou were ordered to create and implement a comprehensive data security plan and also to undertake independent privacy audits every other year for two decades following the order. RockYou also agreed to pay $250,000.
Wyndham Hotels

In its case against Wyndham Hotels, the FTC claimed that Wyndham’s privacy policy misrepresented the security measures that the company and its subsidiaries took to protect consumers’ personal information. The FTC claim stated that this failure led to fraudulent charges to customers resulting in the loss of millions of dollars. The FTC alleged that breaches took place on three separate occasions and that Wyndham took no further action to secure their servers after the first breach, resulting in the further significant theft of data and fraud on the following two occasions.

PLS Financial Services

The FTC charged PLS (Payday Loan Store) with failing to take reasonable measures to protect consumer information. This failure resulted in the disposal of documents containing sensitive personal identifying information, including sensitive financial information. Further to this, the FTC also alleged that the defendants violated the FTC Act by misrepresenting that they had implemented reasonable measures to protect sensitive consumer information. The company agreed to make a settlement for $101,500 and also agreed to implement and maintain a data security program with independent third-party audits every other year for two decades following the order.

Microsoft

The FTC’s complaint alleged that Microsoft misrepresented security measures on a technology referred to as ‘Passport’. They claimed that Microsoft had failed:

- to implement reasonable and appropriate procedure to prevent unauthorised access;
- to monitor the system for vulnerabilities;
- to record information for security audits.

The FTC charge also alleged that Microsoft collected certain personal information while declaring in its privacy policy that did not collect the information. An agreement was made with Microsoft to the effect that:

- Microsoft would not misrepresent its information practices;
- Microsoft would establish a competent and appropriate security program;
- Microsoft would provide material showing their compliance with the FTC order for a period of five years from the date of the order.
Summary

This article summarises a number of high-profile and recent enforcement actions taken by the FTC (Federal Trade Commission) to enforce the security policies implemented under the FTC Act.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- FTC security enforcement actions (II.A.c.)
COPPA: The Children’s Online Privacy Protection Act

The Children’s Online Privacy Protection Act was passed in 1998 by the FTC to protect the personal information of children. It specifically applies to websites that target children and provides guidelines for the collection, use and disclosure of personally identifiable information of children under the age of 13 who may not understand the dangers of disclosing personal information on the Internet.

A website operator must be concerned with COPPA compliance if:

- The website targets children under the age of 13 through its subject matter, audio/visual content, advertising or use of other child-oriented features.
- The website targets a general audience but has a separate child oriented section.
- The website targets a general audience and children under the age of 13 are known to access the site.
- The website is maintained outside the U.S. but targets children under the age of 13 in the U.S.
- The website is operated by the Federal Government. Under the Office of Management and Budget, the U.S. Federal Government is required to comply with COPPA on all of its websites targeting children.

COPPA Compliance

COPPA primarily uses the fair information practice principles of Notice and Consent to protect children’s information.

In order to comply with COPPA, a website operator must:

1. Provide parents with information about the website’s information collection and privacy practices. A privacy policy must be placed on the home page and on every page where data is collected in order to ensure adequate notice.

2. Obtain verifiable parental consent prior to collecting personal information.

3. Provide parents with a mechanism to access the information on record for their child and the ability to change consent options for future or third party use and disclosure.

4. Participation on the website may not be limited by requiring the collection of information that is not reasonably necessary.

A COPPA compliant privacy notice must include:

- Legitimate contact information for the website operator/data owner
- The type of information that is collected
- How the information will be use
- Notice of any third party disclosure
Verifiable Parental Consent:

Depending on the information that is being collected and its intended use, different levels of parental consent must be obtained.

Prior parental consent is not required to collect a child’s name and email address only if:

- The information is obtained in order to provide notice to the parent or obtain parental consent
- The information is collected to respond once to a specific inquiry by the child and not used for further communications
- The information is used to ensure the safety of a child and is not used for any other purposes
- The information is used to protect the security of the website, protect against liability, participate in a law enforcement investigation or any other matters relating to public safety

In all cases, parental consent should be obtained shortly after the information is collected. If parental consent cannot be obtained, the information may not be used for purposes other than those outlined above and the information must be deleted (with exceptions for ensuring the safety of the child)

Parental Consent for Public Disclosure

If the website publicly links a child’s name or email address with their screen name in chat rooms, message boards, personal home pages, pen pal services or other similar social networking features they must obtain verifiable parental consent of public disclosure. This also applies to site which may disclose personal information to third parties for secondary uses and marketing purposes.

Consent options include:

- A printable form that can be signed then mailed or faxed back to the website operator
- Obtain a parent’s credit card information in connection with a transaction which may include subscription fees, purchases or a credit card processing fee.
- Provide a toll free line staffed by professionals to which parents may call and provide verbal consent
- Obtain consent through an email that contains a digital signature that uses a public key that has been verified by one of the above methods.
Parental Consent for Internal Use

If the website does not publicly disclose the child’s information either through disclosure to third parties or through the posting of information to chat rooms, message boards or similar features then the information will only be used within the site to contact the child.

Consent options include:

- Any of the methods used for public disclosure
- The Email Plus option in which:
  - An initial email is sent containing the privacy notice and asking the parent to respond with a phone, fax or mailing address to confirm consent through one of those methods; or
  - After a reasonable length of time has passed, a second email is sent asking for the parent to confirm consent. The privacy notice should again be included. This email informs the parent that their consent is implicit through their lack of response. The email should provide the parent with information on how to revoke their consent.

Enforcement of COPPA

COPPA is enforced by the Federal Trade Commission and through the a state’s Attorney General’s Office under SEC. 1305. COPPA allows for the creation of Safe Harbor programs which encourages industry self regulations.

There are several online assurance programs that offer a COPPA compliant Safe Harbor Program including:

- TRUSTe
- The Children’s Advertising Review Unit
- The Entertainment Software Rating Board

Unlike other information privacy laws, the FTC has been diligent in enforcing COPPA. It has a history of investigating privacy complaints and taking action against website and companies violating the rule.

Summary

COPPA protects the privacy of personal information for children. It does not prevent children from accessing mature content. COPPA uses parental notice and consent to prevent the wrongful collection and misuse of children’s personal information. Any website that may be frequented by children under the age of 13, must comply with the COPPA ruling if personal information is collected.
CIPP Candidate Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post including:

- Children’s Online Privacy Protection Act of 1998 (II.A.d.)
HIPAA: Health Information Portability and Accountability Act

HIPAA is a sectoral law that was first developed in 1996, to enact several changes in the healthcare industry. Among these changes are a security rule and privacy rule which protect personal health information.

What is Protected Health Information?

Protected Health Information is any personally identifiable health information communicated in any form—oral, paper or electronic—that is maintained by a covered entity as defined by HIPAA (see below.) Personally identifiable health information may include a person's age, gender and other demographic information as well as information about their diagnosis; prognosis; their past, present or future medical health or conditions; and payment for the provision of past, present or future medical care. Any information that may potentially identify an individual personally is considered to be protected health information (PHI.)

Who Must Comply With HIPAA?

In general any entity that handles protected health information must comply with HIPAA regulations. However, the law specifically mentions the following all of which are considered “covered entities”:

Health Care Providers – All hospitals, doctors, nurses, health care workers and any other healthcare service providers

Health Plans– Medicare and Medicaid; private insurance companies; group health plans

Business Associates– Any third part that may handle protected health information as a service, such as billing, data analysis, data aggregation, etc.

The Privacy Rule

The HIPAA Privacy rule attempts to strike a balance between the need for disclosure among health care professionals to ensure quality care, payment and maintain public security, while still protecting the identity and personal health information of the patient.
Under the Privacy Rule a patient has the right to:

- *Notice of a covered entity’s privacy practices* which include the type of information collected and its intended use.
- *Consent or object to the disclosure of protected health information to third parties* other than those disclosures granted to business associates for the rendering of treatment or services. The Privacy Rule requires that a signed authorization from the individual be placed on record for each specific third party with which the patient wishes to share their information.
- *Access and amend their protected health information* that an entity has on record about them. A minimal charge may be assessed to cover expenses associated providing access or changes to the their records.
- *Limited disclosure of protected health information.* Disclosure must be limited to that which is minimally necessary. When a health care provider or plan shares personal health information with a business associate for the purposes of rendering a service, (ie: billing, data analysis, research, etc) the covered entity must ensure that the business associate or third party will maintain the same standards of privacy.
- *Safeguarding of their protected health information.* All entities handling personal health information must maintain the necessary physical, technical and administrative safeguards to protect the confidentiality, integrity and security of the patient’s information.

*Exceptions to the Privacy Rule*

The Privacy Rule makes provisions for the disclosure of protected health information without the limitations outlined above for the following situations:

- Information needed for public health activities and safety
- In coordination with law enforcement of judicial activities and proceedings
- Certain research purposes
- Special Government functions
The Security Rule

HIPAA’s Security Rule deals specifically with the protection of personal health information in its electronic form, which includes data stored on computer hard drives and magnetic or digital storage devices.

The Security Rule requires that covered entities take reasonable measures to:

- Ensure the confidentiality, integrity, and availability of electronic health information
- Protect against the unauthorized access, use or disclosure of protected health information.
- Enforce HIPAA compliance in the work force.

Furthermore the Security Rule requires:

- The creation of an individual entity to be responsible for implementing and enforcing the Security Rule
- Initial and periodic risk assessments to determine the efficacy of current safeguards, evaluate new threats and implement the necessary protections to maintain the confidentiality and integrity of the data.
- The creation of an ongoing training program to educate the workforce on complying with the Security Rule
- The Covered entity to incorporate the Security Rule into Business Associate Contracts to ensure that all business associates maintain an equivalent level of protection.

Summary

The Health Care Portability and Accountability Act (HIPAA) plays a significant role in the protection of the privacy of health information. HIPAA is a complex and far reaching law which pertains all professionals involved in the health care field. Education in HIPAA compliance must be ongoing, and compliance closely monitored to ensure the protection of health information.

CIPP Candidate Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post including:

- Health Insurance Portability and Accountability Act of 1996 (II.B.a.)
**HIPAA Enforcement Process**

The [Health Insurance Portability and Privacy Act](https://www.hhs.gov/hipaa/) was passed in 2003. Since then HIPAA has become one of the most consistently enforced privacy laws to date. Enforcement falls largely to the Department of Health and Human Service’s Office for Civil Rights.

HIPAA legislation is divided between two rules: the Privacy Rule and the Security Rule. The Privacy Rule of HIPAA involves the privacy of protected health information (PHI). Among the protections it provides are the right to access and amend medical records, the right to consent to PHI disclosure, the right to notice of a covered entity’s privacy practices, as well as the safeguarding and limited disclosure of PHI. Enforcement of the Privacy Rule ensures that such rights are protected.

**How Does the OCR Enforce the Privacy Rule?**

The Office for Civil Rights enforces the Privacy Rule through several methods:

- Investigating complaints filed with the OCR
- Conducting compliance reviews of covered entities
- Creating programs for education and outreach
- The most common method of enforcement is the investigation of complaints.

**How Does the OCR Investigate Complaints?**

All complaints filed with the OCR go through an Intake and Review process. If the complaint meets the following criteria, the complaint moves on to the investigation stage:

- The alleged violation occurred after the effective dates of the Privacy or Security Rule.
- The entity against whom the complaint is filed must be considered a **covered entity**
- The alleged complaint must be an activity that would violate the Privacy or Security Rule.
- The Complaint must be filed within 180 days of when then person submitting the complaint became aware of the violation.

If the complaint does not meet all of the above criteria, than no violation of HIPAA is considered to have occurred. If the complaint does meet all of the above criteria, an investigation is launched to determine the veracity of the complaint.
If the complaint involves a possible criminal violation, the investigation is handled by the Department of Justice. If the complaint only involves Privacy or Security Rule violations, it is investigated by the OCR. Depending on the results of the OCR investigation:

- No violation may be found
- A violation may be found and voluntary compliance or corrective action is taken
- A formal finding of violation from the OCR is issued

**Enforcement Statistics**

The Number of HIPAA complaints has increased each year since its institution. In 2008, the OCR received almost 10,000 complaints. On average, around two-thirds of alleged complaints are determined to be violations and resolution action is taken. One-third of alleged complaints either do not meet the criteria to warrant an investigation or the investigation determined that no violation had occurred.

On average the top five complaints filed every year involve:

- Impermissible uses and disclosures
- Safeguards
- Access
- More PHI is collected or used than the minimum necessary
- Improper authorization for disclosure

On average, the top five covered entities that have been found to be in violation of the Privacy Rule include:

- Private Practices
- General Hospitals
- Outpatient Facilities
- Health Plans
- Pharmacies
Summary

The OCR is committed to HIPAA enforcement. All complaints filed with the OCR are reviewed and may be subject to investigation if a violation is suspected. Depending on the severity of the violation, the OCR may need to take enforcement action against an entity to ensure compliance. Such enforcement is costly to both the entity, the U.S. Government and its citizens, so covered entities should review their practices and policies to correct any potential compliance violations.

CIPP Candidate Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post including:

- HIPAA privacy rule (II.B.a.i.)
- HIPAA security rule (II.B.a.ii.)
CIPP Applied: HIPAA & CVS Case Study

While understanding privacy law and how it should be implemented is important, it is equally important to know how such laws are enforced and investigated by the U.S. Government. The following case explains the corrective action the Office for Civil Rights under the Department of Health and Human Services was forced to take to ensure compliance of a covered entity that had significantly and repeatedly violated the Privacy Rule of HIPAA.

Following reports of improper disposal of personal health information (PHI) the OCR launched an investigation into the information practices of CVS Entities in September 2007. Their review found the following:

- Between July 2006 and May 2007 some retail CVS stores placed paper records containing personal health information in open dumpsters where they could be accessed by unauthorized individuals.
- The policies and procedures of CVS Entities prior to November 2006 were not adequate to ensure the security of PHI.
- CVS did not have the appropriate administrative safeguards in place, such as disciplinary action or sanctions policies for members violating privacy and security policies.
- Between April 2003 and November 2006, the training given to employees regarding compliance with the Privacy Rule of HIPAA was insufficient to ensure proper destruction of PHI.

In January 2009 a resolution agreement was reached with the following terms:

- Each CVS entity must designate a Compliance Representative that is familiar with the Privacy Rule in order to ensure compliance with HIPAA and the Corrective Action Plan required by the agreement. The Compliance Representative is in charge of designing or improving policies, procedures, training and internal controls.
- CVS must pay the Department of Health and Human Services $2,250,000 in penalties.
- CVS Entities must agree to implement the Corrective Action Plan outlined in the Resolution Agreement.

The Corrective Action Plan (CAP) for CVS entities involved a number of changes in oversight, policy and training to ensure the adequate protection of PHI. Oversight of implementation of the CAP lasts three years from the effective date of the agreement.

The CAP required the following:

Policies

Development, Improvement and maintenance of privacy policies and procedures that comply with the Privacy Rule of HIPAA and any other relevant privacy regulations.

CVS Entities must submit revised policies within 90 days of the agreement and implement the policies within 60 days of OCR approval.
Policies and procedures must be reviewed annually by the Compliance Representative

Physical and Administrative safeguards to allow the proper disposal of PHI must be implemented

*Employee Policies and Training*

All employees accessing personal health information must receive a copy of the new policies and sign a written agreement saying they understand and agree to abide by the Privacy Rule

Employees that fail to comply with the Privacy Rule must receive disciplinary action

Employees that have access to PHI must receive training appropriate to their level of access regarding proper handling of PHI, including its disposal, as well as the sanctions policies for non-compliance. Training should take place within 30 days of employment. Employees are prohibited from handling PHI before completing their privacy training

A written or electronic account of employee training must be made available to the Office for Civil Rights for inspection

Employees must verify in writing that they have received training and certification must be submitted to the relevant CVS entity within 10 days of certification

Training material must be reviewed annually by the Compliance Representative

*Enforcement*

CVS Entities must develop procedures for internal monitoring of compliance to be approved by the OCR

CVS Entities will use a third party assessor to conduct evaluations of compliance with the Privacy Rule and the CAP. The Assessor must file reports with the OCR and Compliance Representative periodically

The Assessor, Compliance Representative and all CVS Entities must maintain all paper’s related to the Assessor’s reports for inspection upon request by the OCR

CVS entities must develop and internal reporting procedure for approval by the OCR which requires employees to report violations of the CAP to the Compliance Representative as soon as they become aware of the problem

Upon receiving an internal report, the Compliance Representative must investigate the problem immediately

If the investigation determines that a violation has occurred a written report describing the violation and the actions taken by the CVS entity must be submitted to the Assessor and the OCR.
Reporting

Within 150 days of OCR approval of the policies and procedures, the Compliance Representative will file an Implementation Report that includes the following information:

A written attestation from the Compliance Representative stating that CVS is in full compliance with the Privacy Rule and the CAP to the best of their knowledge

A written attestation from the Compliance Representative stating that the workforce with access to PHI have received their initial privacy training certification

A copy of all training materials and a summary of the training program including length, topics and schedules

A written attestation from the Compliance Representative with the contact information for all locations and retail pharmacies stating that all locations are compliant with the CAP within the best of their knowledge

A written attestation from the Compliance Representative stating they have reviewed the Implementation Report and believe the evaluation to be accurate

Periodic reports must also be filed once a year to allow ongoing oversight. The periodic reports require similar information regarding training materials and compliance officer attestations. They also require a summary of all engagement between CVS Entities and the Assessor (ie: financial audits, compliance program engagements) and a summary of any compliance violations committed by a workforce employee. Furthermore, CVS is responsible for maintaining all documents related to the CAP for six years.

Significance of the CVS Enforcement Case

The CVS enforcement case reinforced several important privacy issues:

- All employees handling PHI must receive the proper training in their privacy obligations under HIPAA and other privacy laws. Furthermore they must be held accountable for any violations that occur
- Data destruction requires as much attention to privacy concerns as data in other parts of the data life cycle.
- Though most individuals PHI was not compromised through CVS’s improper disposal of data, it is the potential for such unauthorized use, access, or disclosure which is the real problem being addressed in the Corrective Action Plan.
Summary

The U.S. Government is serious about HIPAA enforcement. Entities handling PII must take the necessary steps to ensure compliance or be faced with much stronger requirements, oversight and costs.

CIPP Candidate Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post including:

- Health Insurance Portability and Accountability Act of 1996 (II.B.a.)
- HIPAA privacy rule (II.B.a.i.)
Health Information Technology for Economic and Clinical Health Act (HITECH Act)

Prior to the HITECH (Health Information Technology for Economic and Clinical Health) Act, there were many cases in which patients’ private and confidential information was compromised without knowledge of the health care provider. These data breaches led to legal complications, damage to the brand image and loss of clientele.

What is the HITECH Act?

Enacted on February 17, 2009, the HITECH Act ensures the privacy and security of patient health information. As part of the American Recovery and Reinvestment Act (ARRA) of 2009, the HITECH Act made significant changes to the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Particularly, the HITECH Act creates new requirements concerning privacy and security for health information that both materially and directly affect more entities, businesses and individuals in various ways not covered by the HIPAA.

Significant Changes

The HITECH Act makes the following specific changes to the HIPAA of 1996:

The definition of “business associates” is expanded to include persons and organizations (e.g. subcontractors) that perform activities which involve the use or disclosure of personally identifiable health information (e.g. claims processing, data analysis, quality assurance, billing, benefit management, and other legal, accounting or administrative functions). In the HITECH Act, “business associates” also includes organizations that transmit protected health information and those that require access on a routine basis to such information.

As of February 17, 2010, HIPAA security standards that apply to health plans and health care providers will directly apply to business associates. This means that they will also be subject to the administrative, physical and technical security requirements of HIPAA. They must also implement the necessary policies and procedures for documenting security activities. Any penalties for violating HIPAA procedures will also apply to “business associates.”

The HITECH Act also establishes new security breach notice requirements. As of September 2010, health plans and health care providers that access, maintain, retain, modify, record, store, destroy or otherwise hold, use or disclose unsecured protected health information and discovers a breach must notify each individual who has been affected by the breach. Business associates will also need to give notice of such data breaches. According to the Act, notices must be provided by first-class mail to individuals at their last known address, or if specified by the individual, by e-mail.
As of February 17, 2010, individuals are entitled to electronic copies of their health information from any health plan or health care provider that uses or maintains electronic health records. Individuals should be able to direct the health plan or health care provider to transmit the copy directly to a designated individual. Fees for this service should also be kept to a minimum.

Six months after such regulations have been enacted, the HITECH Act prohibits a health plan, health care provider or business associate from receiving payment for an individual’s protected health information, without prior authorization from the individual.

**HITECH Act Breach Notifications**

The HITECH Act includes notable breach notification regulations that require health care providers and other HIPAA-covered entities to notify affected individuals of a data security breach, as promptly as possible. In addition, the [Department of Health and Human Services](https://www.hhs.gov) (HHS) Secretary and the media must also be notified if the breach affects more than 500 individuals. Breaches that affect less than 500 individuals will be reported to the HHS secretary annually.

**According to Robinsue Frohboese**, the Acting Director and Principal Deputy Director of OCR:

“This new federal law ensures that covered entities and business associates are accountable to the Department and to individuals for proper safeguarding of the private information entrusted to their care. These protections will be a cornerstone of maintaining consumer trust as we move forward with meaningful use of electronic health records and electronic exchange of health information.”

**HITECH Act-Compliance Checklist**

**According to Adam Greene**, former HIPAA enforcer, there are a number of elements that an entity must secure in order to be HITECH-compliant:

- Have you formally designated a person/position as your organization’s privacy and security officer?
- Do you have documented privacy and information security policies and procedures?
- Have they been reviewed and updated, where appropriate, within the last six months?
- Have the privacy and information security policies and procedures been communicated to all personnel, and made available for them to review at any time?
- Do you provide regular training and ongoing awareness communications for information security and privacy for all your workers?
- Have you done a formal information security risk assessment in the last twelve months?
- Do you regularly make backups of business information and have documented disaster recovery and business continuity plans?
Do you require all types of sensitive information, including personal information and health information, to be encrypted when it is sent through public networks and when it is stored on mobile computers and mobile storage devices?

Do you require information (in all forms) to be disposed of through secure methods?

Do you have a documented breach response and notification plan, as well as a team equipped to support the plan?

Summary

This article takes a look at the HITECH (Health Information Technology for Economic and Clinical Health) Act of 2009, which made significant changes to the HIPAA (Health Insurance Portability and Accountability Act) of 1996. Notably, the HITECH Act made mandated specific procedures for responding to data security breaches, including particular breach notification procedures. The article includes a list of significant changes made by the Act, as well as a compliance checklist for covered entities.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Health Information Technology for Economic and Clinical Health Act of 2009 (II.B.b.)
CIPP Applied – The Cost of Data Breaches

A recently-released report revealed that many health care organizations in the United States experience undetected data breaches, which cost up to $1 million per organization per year, or about $6 billion annually. The failure of organizations to prevent or detect patient data breaches may result in medical identity theft, financial identity theft and unintentional disclosure of medical facts.

In Brief

The report, entitled the Benchmark Study on Patient Privacy and Data Security, was published by the Ponemon Institute and ID Experts in November 2010. The study was based on findings from 65 health care organizations (mainly hospitals) and included an examination of each organization’s privacy and data protection compliance activities; policies; program management activities; security technologies; security governance practices; and compliance with the mandates of the HITECH Act of 2009.

The major findings of the report are briefly outlined below:

Data breaches cost the US health care system billions of dollars each year. The study revealed that the economic impact of data breach incidents amounted to over $2 million, over a two-year period.

The majority of health care organizations have undetected patient data breaches. Organizations participating in the study reported they had inadequate resources (71%); few appropriately trained personnel (52%); and insufficient policies and procedures in place (69%) that could quickly and effectively prevent/detect patient data loss. It was shown that data breaches went undetected due to the lack of preparation and staffing.

Patient data protection is not a priority in health care organizations. 70% of hospitals participating in the study responded that protecting patient data was not one of their top priorities. 67% of the organizations hired less than two staff members dedicated to data protection management. At many organizations, the patients were the first to detect a disturbingly high number of breaches (41%). This means that sensitive data was being unknowingly exposed until the individuals detected the breach.

Despite recently-enacted federal regulations, the security of patient records has not improved. Acts supporting the privacy security of medical information, such as the HITECH Act of 2009 and the HIPAA of 1996 have not resulted in stronger safeguards for patient data. According to the study, 71% of respondents did not believe that these federal regulations have sufficiently improved the management of patient records.
What is the HITECH Act?

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 was enacted as part of the American Recovery and Reinvestment Act of 2009. It was designed to address privacy and security concerns regarding the electronic transmission of health information. With the HITECH Act, starting in 2011, a physician is eligible to receive up to $44,000 in incentives for “meaningful use” of an electronic health record (EHR).

The HITECH Act also extended the Privacy and Security Provisions of the HIPAA to business associates of covered entities, which include criminal and civil penalties. The Act imposes new breach notification requirements on the following entities:

- Covered entities
- Business associates
- Vendors of personal health records
- Related entities

Finally, the HITECH Act implements rules regarding disclosures of a patient’s health information. Disclosures include information that is used for treatment, payment and health care operations when the health care provider is using an EHR.

Moving to EHR

The majority of respondents in the Ponemon study believed that making the switch to electronic health records (EHR) would make patient data more secure. EHRs are longitudinal electronic records of patients’ health information. They are both generated and maintained within a health care institution, such as a hospital, integrated delivery network, clinic or physician’s office.

Such records would include:

- Progress notes
- Patient’s demographics
- Past medical history
- Immunizations
- Health Problems
- Medications
- Vital signs
- Laboratory data
- Radiology reports

Proponents argue that implementation of EHR processes and systems will help to provide additional functionality (e.g. interactive alerts, interactive flow sheets, tailored order sets), which may not be possible with traditional, paper-based systems. Other major benefits of EHRs include:
According to a recent study conducted by researchers at the Stanford University School of Medicine, EHRs did little to improve the quality of health care. This was based on data from almost 250,000 patient visits, between 2005 and 2007. Although the federal government’s American Reinvestment and Recovery Act of 2009 allotted $19.2 billion for health information technology, specifically for the adoption of EHRs, there has not yet been evidence of positive impact.

Summary

The article takes a look at the 2010 Benchmark Study on Patient Privacy and Data Security, conducted by the Ponemon Institute. The study revealed that data breaches were costing hospitals across the US up to $6 billion each year. Breaches of patient information are largely undetected by the organization, due to lack of priority, resources, preparation and staffing for privacy and security management. The article then examines the HITECH Act (the Health Information Technology for Economic and Clinical Health Act), passed in 2009 to strengthen privacy and security safeguards for health information. One contentious issue is the adoption of electronic health records (EHRs). Although the federal government has created economic incentives for the implementation of EHR systems, researchers have found them ineffective at improving the quality of health care.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Health Insurance Portability and Accountability Act of 1996 (II.B.a.)
- Health Information Technology for Economic and Clinical Health Act (II.B.b.)
CIPP Applied – WPF’s Medical Identity Theft Map

The World Privacy Forum (WPF) has released a medical identity theft map, an interactive map highlighting the location of all medical ID theft complaints collected from 2008- February 12, 2009 by the Federal Trade Commission (FTC). The map enables users to interactively view one year of medical identity theft activity in the US, based on FTC complaints.

In order to create this tool, the WPF analyzed the FTC’s Consumer Sentinel incident reports. As such, the data is consumer-reported, thus does not represent a final, definitive picture of medical identity theft. However, the map reveals a significant geographic clustering of medical identity theft in the states of Florida, California (in particular southern California), New York, Arizona, and Texas.

A closer look at medical identity theft...

Medical identity theft takes place when someone uses a person’s name and sometimes other parts of their identity – for instance insurance information – without the individual’s knowledge or consent, in order to access medical services or goods, or uses the person’s identity information make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries put into existing medical records, sometimes involving the creation of fictitious medical records in the victim’s name.

According to the FTC, it’s important to read medical and insurance statements regularly and completely, as these can indicate warning signs of identity theft. In particular, it’s important to read the Explanation of Benefits (EoB) statement or Medicare Summary notice sent by the health plan after treatment. Other signs of medical identity theft include:

- A bill for medical services you didn’t receive
- A call for a debt collector about a medical debt you don’t owe
- Medical collection notices on your credit report you don’t recognize
- A notice from your health plan saying you have reached the benefit limit
- A denial of insurance because your medical records show a condition you don’t have

Unfortunately, medical identity theft is an issue that has been poorly researched and under-reported until now. According to the World Privacy Forum,

“Medical identity theft is a crime that can cause great harm to its victims. Yet despite the profound risk it carries, it is the least studied and most poorly documented of the cluster of identity theft crimes. It is also the most difficult to fix after the fact, because victims have limited rights and recourses. Medical identity theft typically leaves a train of falsified information in medical records that can plague victims’ medical and financial lives for years.”

As such, the WPF has researched and published the first major report about medical identity theft, entitled Medical Identity Theft: The Information Crime That Can Kill You.
Within the US, there are a number of relevant laws surrounding health privacy. The Health Information Portability and Accountability Act (HIPAA) is the most important federal health privacy law, however, there are others which also affect medical privacy. These include:

- Privacy Act of 1974
- Confidentiality of Alcohol and Drug Abuse Patient Records Regulations
- Family Educational Rights and Privacy Act (FERPA)
- Americans with Disabilities Act (ADA)
- Genetic Information Nondiscrimination Act (GINA)

Summary

This article introduces the World Privacy Forum’s (WPF) medical identity theft map, an interactive map that locates medical identity theft complaints collected from 2008-9 by the Federal Trade Commission. The article also provides a definition of “medical identity theft,” as well as resources for victims of medical ID theft.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US), a privacy professional should be comfortable with topics related to this post, including:

- Limits on private sector collection and use of data – medical (II.B.)
Fair Credit Reporting Act (FCRA)

The Fair Credit Reporting Act (FCRA) was enacted in 1970 to promote accuracy, fairness, and the privacy of personal information assembled by Credit Reporting Agencies (CRAs). The Act was passed largely to address the credit reporting industry in the US that compiled “consumer credit reports” and “investigative consumer reports” on individuals. It represents the first federal law to regulate the use of personal information by private businesses.

What does the FCRA do?

The federal FCRA promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies.

Credit reports can include a wide range of sensitive personal information and are used to evaluate an individual’s ability to participate in many different activities. They are subject to regulations within a framework of Fair Information Practices.

Here is a summary of the major rights protected by the FCRA:

- You must be told if the information in your file has been used against you. Anyone who uses a credit or consumer report against you must provide you with the name, address, and phone number of the agency that provided the information.
- You have the right to know what is in your file. You are entitled to a free file disclosure if:
  - A person has taken adverse action against you because of information in your credit report.
  - You are the victim of identity theft and place a fraud alert in your file.
  - Your file contains inaccurate information as a result of fraud.
  - You are on public assistance.
  - You are unemployed, but expect to apply for employment within 60 days.
  - Also, all consumers are entitled to a free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies.
- You have the right to ask for a credit score. Individuals may request a credit score from consumer reporting agencies, at a cost.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
Problematic information must be removed or corrected, usually within 30 days. A CRA may continue to report information it has verified as accurate.

- Consumer reporting agencies may not report outdated negative information. CRAs may not report negative information over 7 years old, or bankruptcies that are more than 10 years old.
- Access to your file is limited. Information may only be provided if it is necessary (e.g. for an application with a creditor, insurer, employer, landlord, etc.).
- You must give your consent for reports to be provided to employers. Consent must be in written form and provided to the employer (except for those working in the trucking industry).
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report. Unsolicited “prescreened” offers must include a toll-free phone number for individuals to call, should they choose to remove their name and address from the lists.
- You may seek damages from violators. If a CRA, or in certain cases, a user of consumer reports or a furnisher of information to a CRA, violates the FCRA, individuals may be able to sue in state or federal court.
- Identity theft victims and active duty military personnel have additional rights.

It’s also important to note that states have the authority to enforce the FCRA and many states have their own consumer reporting laws which may be even more stringent than the federal Act.

**FCRA Basics**

The FCRA establishes rights and responsibilities for “consumers,” “furnishers,” and “users” of credit reports:

- Consumers – individuals
- Furnishers – entities that send information to CRAs regarding credit worthiness in the normal course of business
- Users – entities that request a report to evaluate a consumer for some purpose

A consumer reporting agency (CRA) is an entity that assembles and sells credit-related and financial information about individuals. There are three national CRAs in the US:

1. Experian
2. Trans Union
3. Equifax
There are also smaller, regional credit reporting agencies. Inspection bureaus (i.e. companies that sell information to insurance companies and assist in background checks), tenant screening and check approval companies are often considered to be CRAs as well.

What's in a CRA?

Consumer credit reports may contain information on financial accounts, including credit card balances and mortgage information. Credit reports may be used for evaluating:

- Eligibility (e.g. for credit, insurance, employment, tenancy)
- The ability to pay child support
- Professional licensing (e.g. to become an attorney)
- For any purpose that a consumer approves

Consumer credit reports contain basic identifying information (e.g. name, address, previous address, SSN, marital status, employment information, number of children), as well as the following information:

- Financial information (e.g. estimated income, employment, bank accounts, value of car and home)
- Public records information (e.g. arrests, bankruptcies, tax liens)
- Tradelines (e.g. credit accounts and their status; payment habits on credit accounts)
- Collection items (i.e. whether there are unpaid or disputed bills)
- Current employment and employment history
- Requests for the credit report (i.e. the number of requests for the individual’s report and the identity of the requestors)
- Narrative information (i.e. a statement by the individual, or the furnisher regarding disputed items on the credit report)
- Health information

Summary

The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness and privacy of information in the files of consumer reporting agencies. This article provides a summary of the basic rights under the FCRA as well as a definition of the most important terms.
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Fair Credit Reporting Act of 1970 (II.C.a.)
Fair and Accurate Credit Transactions Act of 2003 (FACTA)

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) was enacted in 2003 and outlined specific document destruction rules that would come into effect two years later. The FACTA also amended the existing Fair Credit Reporting Act (FCRA), providing consumers, companies, consumer reporting agencies and regulators with new tools to expand consumer access to credit, enhance the accuracy of consumer financial information and help fight identity theft. The FACTA is administered by the Federal Trade Commission (FTC).

FACTA Basics

The FACTA applies to any person or company that maintains or retains consumer information, such as consumer reports, for a business purpose. Examples of those who would be impacted by the FACTA include:

- Consumer reporting agencies (CRAs)
- Resellers of consumer reports
- Lenders
- Insurers
- Employers
- Landlords
- Government agencies
- Mortgage brokers
- Auto dealers
- Waste disposal companies

FACTA added new sections to the existing federal Fair Credit Reporting Act (FCRA), intended primarily to help consumers combat identity theft. FACTA is also concerned with issues such as accuracy, privacy, limits on information sharing and new consumer rights to disclosure.

FACTA includes a specific rule regarding the proper disposal of consumer report information and records. The purpose of this rule is to reduce the risk of identity theft and other consumer harm from the inappropriate disposal of a consumer report, or records derived from such reports. The FACTA rule states:

“Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.”
Helping out Identity Theft Victims

The FACTA includes a number of significant provisions aimed to provide assistance to victims of identity theft. These provisions include:

- **Free credit reports** – Consumers will receive one free credit report every 12 months from each of the “big three” national credit bureaus.
- **Fraud alerts** – Victims of identity theft can place a fraud alert on their accounts, which are effective for 90 days, but may be extended (with proof of identity theft) for a period of seven years. Active duty alerts allow active duty military personnel to place a notation on their credit reports to alert potential creditors to possible fraud.
- **Truncation** – Systems that print payment card receipts must employ PAN truncation so that the consumer’s full account number is not visible on the slip.
- **Available information** – The FACTA includes provisions that help victims access copies of the imposter’s account application and transactions.
- **Collection agencies** – Once creditors are notified of debts due to identity theft, they are not permitted to sell the debt or place it for collection.
- **Red flags** – Financial institutions, creditors and other businesses that rely on consumer reports are required to detect and resolve fraud by identity theft. FACTA includes Red Flag Guidelines and requirements for credit and debit card issuers to assess the validity of a change of address request. The Act also outlines procedures to reconcile different consumer addresses.

FACTA & Workplace Privacy

The FACTA sets a new standard for what is known as “employee misconduct investigations.” Such investigations are conducted by a third-party contracted by the employer, if there is reason to suspect an employee of:

- Misconduct relating to the terms of employment
- A violation of federal, state, or local laws or regulations
- A violation of any preexisting written policies of the employer
- Noncompliance with the rules of a self-regulatory organization

An employer who suspects an employee of misconduct does not have to give notice or get the employee’s permission to conduct a misconduct investigation. Like other inquiries covered by the FCRA, this only applies if the employer hires an outside party to conduct the investigation.

The findings of employee misconduct investigations cannot be disputed under the FCRA dispute procedure. These types of investigations have deliberately been removed from the definition of “consumer report,” thus the usual protections that apply to a consumer report conducted for employment purposes do not apply to employee misconduct investigations.
Summary

The Fair and Accurate Credit Transactions Act (FACTA), enacted in 2003, amended the existing Fair Credit Reporting Act of 1970 (FCRA). It also included several important provisions to help consumers avoid and respond to identity theft crimes.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Fair and Accurate Credit Transactions Act of 2003 (II.C.b.)
The Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999 applies to the financial sector. GLBA repealed part of the Glass-Steagall Act of 1933 which required financial institutions to be restricted to acting as either an investment bank, a commercial bank, or an insurance company. With the repeal, financial institutions were allowed to merge these activities under one company or financial group.

The Gramm-Leach-Bliley Act also created a Privacy Rule to regulate the collection, use and disclosure of customer’s financial information. Furthermore it created a Safeguards rule which requires security measures to be implemented to protect consumer information from unauthorized access and disclosure.

Who must comply with the Gramm-Leach-Bliley Act?

All financial institutions must comply with the act, even those that do not disclose private financial information. Privacy policies and security safeguards must be in place regardless of the disclosure practices of a company. The Safeguards Rule applies not only to financial institutions but all entities handling financial information such as Consumer Reporting agencies.

The Privacy Rule

The Privacy Rule of the GLBA protects the privacy of customers of financial institutions and their non-public information. A customer is defined as having a long-term relationship with a financial institution such as the lending of a mortgage, a loan or insurance. Only information that is not considered part of the public record is protected under the Privacy Rule. Non-public information includes information provided by the consumer in connection with an application for, or receipt of, a product or service with the financial institution.

Under the Privacy Rule:

- A customer must receive a copy of the financial institution’s privacy notice upon entering the relationship and once every year for the duration of the relationship. A new copy of the notice must be provided upon the modification of any of the privacy policies.
- The Privacy Notice must contain the type of information collected by the financial institution how it is used, notice of possible third party disclosures and a statement regarding the safeguarding of their personal information.
- The Privacy Notice must contain a statement notifying the customer of the opportunity to opt out of disclosure of information to unaffiliated third parties so as to comply with the Fair Credit Reporting Act.
- Financial Institutions are prohibited from sharing customer account numbers with non-affiliated third parties.
Title V of the Gramm-Leach-Bliley Act provides regulations for the disclosure of information to third parties:

- Financial institutions may share any customer information with affiliated third parties
- Financial institutions may share customer information with nonaffiliated third parties only if an opt out notice has been given to the customer and they have not exercised their right to stop nonaffiliated disclosures.

The Safeguards Rule

The Safeguards rule requires all financial institutions to have security plans in place to ensure the confidentiality and integrity of customer data. An Information Security Plan must make use of:

- Administrative safeguards, such as employee oversight and training;
- Physical safeguards, such as restricted access to hardware and disaster recovery plans;
- Technical safeguards such as firewalls, encryption, access controls and secure computer networks.
- Safeguards must be implemented in proportion to the scope of and risk to the institution and the information it handles.

Furthermore, the Safeguards rule requires that an employee oversee the development and coordination of security in the institution.

Summary

The Gramm-Leach-Bliley Act made major changes to the financial sector, particularly with regard to the protection of customer information. Though the GLBA pertains mostly to financial institutions engaged in long term relationships with individuals, it is important for all business owners to understand how financial information is protected and where their organization, and the financial information they collect, fits under financial sector privacy law.

CIPP Candidate Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post including:

- Financial Services Modernization Act of 1999 (II.C.c.)
Red Flags Rule: Delayed Enforcement & Amendments

It has been estimated that up to nine million Americans are victims of identity theft each year. However, consumers are largely unable to prevent or detect identity theft, rather depend on businesses and organizations to spot anomalies. For this reason, the Red Flags Rule was developed in order to spot warning signs (“red flags”), prevent identity theft and limit the damage that may be done. This article takes a closer look at the Red Flags Rule, as well as a recently introduced bill that may have important implications for the Rule.

Background: The Red Flags Rule

The FTC’s Identity Theft Red Flags Rule became effective on January 1, 2008. It was then delayed and the FTC set a target date for enforcement as of December 31, 2010. The reason for the delay was to give Congress enough time to finalize legislation limiting the scope of businesses covered by the Red Flags Rule. Any legislation passed by Congress limiting the scope of the Red Flags Rule with an effective date earlier than December 31, 2010 will be enforced by the FTC as of that date.

The Red Flags Rule was developed under the Fair and Accurate Credit Transactions Act (FACTA), which requires the FTC, amongst other agencies, to develop regulations that require creditors and financial institutions to address the risk of identity theft. FACTA addressed the need for businesses to be involved in identity theft protection. It obliges financial institutions, creditors and other businesses that use consumer reports to detect and resolve identity theft-related fraud.

What are the “red flags”?

The Red Flags Rule requires businesses and organizations to implement a formal Identity Theft Prevention Program. Such a program should detect the “red flags,” or warning signs that identity theft may be taking place. Red flags are defined as “suspicious patterns or practices, or specific activities, that indicate the possibility of an identity theft.”
The Rule sets out that the Identity Theft Prevention Program be composed of the following four elements:

1. **Identify relevant red flags**: The Program should be made up of policies and procedures for identifying red flags during day-to-day operations.

2. **Detect red flags**: The Program should be designed to detect the red flags that have been identified.

3. **Prevent and mitigate identity theft**: The Program must outline appropriate actions for dealing with red flags.

4. **Update the Program**: The Program should periodically be re-evaluated, in order to appropriately address the evolving threat of identity theft.

When identifying red flags, it is important for the business or organization to consider the types of accounts that it offers or maintains; how these accounts are opened; and how customers have access to these accounts. There are five categories of common red flags, as outlined below:

- **Alerts, Notifications and Warnings from a Credit Reporting Company.** Changes in credit reports or credit activity may point towards identity theft. Such changes may include: a fraud alert on a credit report; notice of address discrepancy; or a notice of a credit freeze when a credit report is requested.
- **Suspicious Documents.** Examples include: altered/forged identification; inconsistencies between the person presenting the ID and the photo/physical description on the ID; or applications that appear altered/forged.
- **Suspicious Personal Identifying Information.** This may include: inconsistencies with other personally identifying information; fraudulent addresses, phone numbers, etc.; contact information that have been used by other individuals to open accounts; or a person who is unable to provide authenticating information.
- **Suspicious Account Activity.** Usage of the account can also signal fraud. For example: an account that is being used inconsistently; new accounts that are used in ways generally associated with fraud; inactive accounts are suddenly being used; or information regarding unauthorized charges on the account.
- **Notice from Other Sources.** Information that an account is being used fraudulently may come from customers, victims or identity theft, law enforcement authorities, etc.
Who is covered by the Red Flags Rule?
The Red Flags Rule applies to financial institutions and creditors. Under the Rule, a financial institution includes:

- A state or national bank
- A state or federal savings and loan association
- A mutual savings bank
- A state or federal credit union
- Any entity that directly or indirectly holds a transaction account that belongs to a consumer

Under the rule, creditors are defined as:

- Businesses or organizations which provide goods or services to customers first and allow them to pay later. Examples include: utilities, health care providers, lawyers, accountants and telecommunications companies.
- Businesses or organizations that grant or arrange loans; extend credit; and make credit decisions. Examples include: finance companies, mortgage brokers, auto dealers, retailers that offer financing and retailers that collect/process credit applications for third parties.
- Anyone who participates in decisions to extend, renew, continue credit, or in setting the terms of credit. Examples would include third-party debt collectors who negotiate the terms of the debt.

According to the FTC, businesses or organizations that have a low risk of identity theft are permitted to complete a do-it-yourself prevention guide. Risk is assessed through the following questions:

1. Do you know your clients personally?
2. Do you usually provide your services at customers’ homes?
3. Have you ever experienced an incident of identity theft?
4. Are you in a business where identity theft is uncommon?

H.R. 6420
The Red Flag Program Clarification Act of 2010 (also referred to as H.R.6420) was first introduced on November 17, 2010 by Representative John Adler (D-NJ). The H.R. 6420 was drafted to “amend the Fair Credit Reporting Act (FCRA) with respect to the applicability of identity theft guidelines to creditors.” The objective of the bill is to limit the scope of the FTC Identity Theft Red Flags Rule.

The H.R. 6420 would limit the definition of “creditor” to exclude those “that advance funds on behalf of a person for expenses incidental to a service provided by the creditor to that person.” This definition would also apply to other creditors, if “such creditor offers or maintains accounts that are subject to a reasonably foreseeable risk of identity theft.” The H.R. 6420 was developed in order to respond to concerns that the current definition of “creditor” extends the scope of the
Red Flag Rule inappropriately. A number of members of Congress voiced their concern that the Rule may include attorneys, law firms and health providers.

Summary
This article takes a look at the Red Flag Rule, which was developed under the FACTA (Fair and Accurate Credit Transactions Act). The purpose of the Rule was to ensure that businesses and organizations were taking the appropriate steps to prevent and respond to identity theft. Although the Rule became effective on January 1, 2008, its enforcement date has been repeatedly been postponed. Currently, the FTC must begin enforcing the Rule on December 31, 2010. This delay is due to the amendments that have been made to the Rule, the most recent being the H.R. 6420, or the Red Flag Program Clarification Act of 2010.

CIPP Exam Preparation
In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Red Flags Rule (II.C.d.)
Dodd-Frank Wall Street Reform and Consumer Protection Act

The Dodd-Frank Wall Street Reform and Consumer Legislation Act is legislation passed in 2010 by the US Congress with the goal of restoring “financial stability in the US by improving accountability and transparency in the financial system, to end the ‘too-big-to-fail’ policy, to protect the American taxpayer by ending enormous bailing and to protect consumers from abusive financial services practices and for other purposes.” The Act was drafted as a result of the 2008 financial crisis and impacts all major sectors of the financial services industry, including banks, thrifts, financial holding companies, mortgage brokers, etc.

The general theme of the Act is to provide financial regulators with information to monitor and understand the risks of the financial system so that measures can be taken to control them. Previously, federal regulators only had direct supervisory powers over depository institutions, their holding companies and their subsidiaries. This lack of power was demonstrated by the failure of the US government to intervene prior to the collapse of Lehman Brothers.

Following enactment, Congress decided that the Act was to become effective in stages, with regulators drafting rules for 6 to 18 months after the enactment.

Although the Act reflects the fact that private funds such as hedge funds were not the primary cause of the financial crisis, their increasing importance to the global financial system meant that the drafter imposed certain recordkeeping and reporting requirements on fund managers.

Provisions of the Act

Some of the more important provisions of the Dodd-Frank Act include:

- The creation of the Bureau of Consumer Financial Protection (BCFP), a new independent consumer watchdog that is part of the Federal Reserve Board (FRB). This office has the authority to ensure consumers get clear accurate information on financial products, along with protecting them from hidden fees and deceptive practices.
- Grants the US Department of the Treasury, Federal Deposit Insurance Corporation (FDIC) and the FRB powers to seize, close and wind down ‘too big to fail’ financial institutions in an orderly fashion. This power also seeks to limit the size of any one financial institution. The FRB is prohibited from approving mergers or acquisitions that would result in the total consolidated liabilities of the resulting company exceeding 10% of the aggregated consolidated liabilities of all financial companies as of the end of the preceding calendar year.
- Establishes a new Financial Stability Oversight Council (FSOC), charged with identifying and responding to emerging risks throughout the financial system, composed primarily of federal financial services regulators and chaired by the Secretary of the Treasury.
Department. The Council is also empowered to identify ‘systematically important’ non-bank financial companies.

- Increases the powers of the Federal Reserve Board, giving it responsibilities for overall risk management requirements and for prompting corrective action to apply to systemically important financial institutions. The Act also abolishes the Office of Thrift Supervisions and redistributes its powers to the Federal Reserve, the Comptroller of the Currency and the FDIC.

- Establishes the Federal Insurance office (FIO), which participates in the oversight and coordination between the US insurance market and the international insurance market, for the purpose of pursuing greater uniformity of the insurance regulatory environment in the US. Its main duty is to collect and analyze data for the insurance industry.

- Establishes the Office of Financial Research (OFR) that is tasked with gathering information from financial market participants. The OFR has substantial powers backed by subpoenas and all data collected is subjected to the Freedom of Information Act.

- Eliminate existing loopholes that allow risky and abusive practices to carry on unregulated e.g. over-the-counter derivatives, asset-backed securities, hedge funds etc.

- Empowers regulators to pursue cases of fraud, conflicts of interest and manipulation of the system that benefits special interests.

- The Volcker Rule requires regulators to implement regulations for banks, their affiliates and holding companies to prohibit proprietary trading, investment in and sponsorship of hedge funds and private equity funds. It also requires systemically important non-bank financial companies to carry additional capital and comply with other quantitative limits on such activities. However, the Volcker Rule includes certain exceptions such as US government investments or investments in small business investment companies.

- The Collins Amendment imposes enhanced risk-based standards and capital requirements for systemically important companies (bank holding company with $50b or more in assets or identified as systemically important by the FSOC). The Amendment also establishes a leverage ratio to deduce the build-up of leverage in the overall system.

- The activities of swap dealers or major swap participants (MSPs) will be subject to greater oversight and regulation. This includes regulations on registrations of such dealers and participants and that all clearable swaps must be executed through a regulated exchange or central clearing entity.

Conclusion

The Dodd-Frank Act is significant legislation towards changing the regulatory system. However, it is unlikely that once piece of legislation will be able to confront all issues raised by the crisis. Loopholes will exist and banks will attempt to exploit them so it is important that the regulators ensure that the rules are adhered to. There is no guarantee that the Dodd-Frank Act will prevent a financial crisis in the future but is, at the very minimum, a step closer to a stronger and better regulated economy.
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Dodd-Frank Wall Street Reform & Consumer Protection Act of 2010 (II.C.e.)
The Consumer Financial Protection Bureau

Created by the Dodd-Frank Act Wall Street Reform and Consumer Protection Act 2010, the Consumer Financial Protection Bureau (CFPB) is a new independent consumer watchdog that is part of the Federal Reserve Board (FRB). The CFPB is authorised to exercise primary supervisory responsibility over large banks and other large non-bank institutions that provide financial products or service, for the purposes of ensuring that consumers get accurate information on financial products, along with protecting them from hidden fees and deceptive or abusive practices.

The CFPB is headed by an independent director that is appointed by the President and confirmed by the Senate. The director serves a five year term. The Bureau has a dedicated budget that is paid by the Federal Reserve and the amount must not exceed a percentage of the Fed’s earning, an up to $200 million in appropriations from 2010-2014.

The Dodd-Frank Act provides the CFPB with the authority to issue and interpret many of the federal consumer protection laws. Further, state attorney generals have been empowered with expanded authority to litigate against national banks and federal thrifts.

One of the main advantages of the CFPB is that it consolidates consumer protection powers within one office. Prior to the Dodd-Frank Act, up to seven agencies had responsibility for the federal protection of consumer finance, resulting in oversights and vast sectors of the market not being regulated at all. Many of these agencies were federal banking agencies that were not centrally focused on consumer protection, but rather on the solidity of financial institutions.

The powers and responsibilities of the CFPB include:

- **Rulemaking, supervision and enforcement for Federal consumer financial protection laws** - The Bureau has the power to autonomously write rules for consumer protection that governs all financial institutions that offer consumers financial services or products.
- **Restriction on unfair, deceptive or abusive acts or practices** – The Bureau has the power to prevent a financial institution from engaging in or committing such an act or practice in connection with a transaction for a consumer financial product or service. The Bureau also has the authority to ensure that the information relevant to the purchase of such products is disclosed to consumers in plain language in a manner that ensures that the consumers understand that costs, benefits and/or risks associated with the product or service.
- **Taking consumer complaints** – The Bureau’s powers consolidate and strengthen the consumer protection responsibilities that were previously powers of the disbanded Office of Thrift Supervision. It has led to the creation of a national consumer complaint hotline so that consumers will have a single toll-free number to report problems with financial products and services.
- **Promoting financial education** – The Bureau is charged with the creation of a new Office of Financial Literacy.
- **Protection of Small Businesses** – The Bureau is tasked with ensuring that small businesses are not unintentionally regulated by them, excluding the businesses that meet the standards required for regulation.

- **Examination and enforcement** – The Bureau has the authority to examine and enforce regulations for banks and credit with assets of over $10 billion and other non-bank large financial companies. The Bureau is charged with enforcing a number of financial laws, including The Truth in Lending Act, The Fair Credit Reporting Act, The Real Estate Settlement Procedures Act and The Equal Credit Opportunity Act. The Bureau also enforces a number of Federal Trade Commission rules, such as the rules regarding cooling-off periods for telemarketing and door-to-door sales.

- **Working with Bank Regulators** – The Bureau must coordinate with regulators when examining banks to prevent undue regulatory burden. It must also coordinate with regulators as well as the SEC and CFTC to promote consistent regulatory rulemaking.

- **Creation of a Consumer Advisory Board** – The Director of the CFPB must take steps to create a Consumer Protection Board to advise and consult with the Director on a variety of consumer financial issues. The Board will be required to have a minimum of 16 members and must have at least two annual meetings. Nominees to the board must have a background in consumer protection or financial services protection.

To implement these provisions, the CFPB tends to follow a number of approaches including a market-based approach, evidence-based analysis, the facilitation of robust public participation through innovative technologies and transparency and learning from historical approaches and borrowing best-practices from other agencies. These principles are aimed to ensure that the CFPB’s work promotes fair, transparent and competitive markets for consumer financial products and services and empowers consumers to take more control of their financial affairs.

**Summary**

This article looks at the Consumer Financial Protection Bureau (CFPB), a new independent consumer watchdog that is part of the Federal Reserve Board (FRB). The CFPB is authorised to exercise primary supervisory responsibility over large banks and other large non-bank institutions that provide financial products or service, for the purposes of ensuring that consumers get accurate information on financial products, along with protecting them from hidden fees and deceptive or abusive practices.

**CIPP Exam Preparation**

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Consumer Financial Protection Bureau (II.C.f.)
Family Educational Rights and Privacy Act of 1974

The Family Educational Rights and Privacy Act of 1974 (FERPA) (also referred to as the Buckley Amendment) is a US Federal law that protects the privacy of student education records i.e. records, files, documents and other materials containing information directly related to a student that are maintained by an educational institution. These may include transcripts, class schedules, class rolls and academic history reports. FERPA applies to all schools that receive funds under an applicable program of the US Department of Education. Most private and parochial schools do not receive these funds and are thus not subject to FERPA.

The rights included in FERPA generally apply to the parents of the child until the child reaches the age of 18 or attends a school beyond high school level, at which time the rights transfers to the student. The FERPA affords full rights to either parent unless evidence is provided that there is a court order, state statute, or other legally binding document that specifically revokes these rights. Step-parents also have rights under FERPA if the step-parent is present in the home on a day-to-day basis. Students to whom the rights are transferred to are referred to as ‘eligible students’. Records can still be disclosed to parents without consent if the student is a dependent for Federal income tax purposes.

Generally, FERPA allows educational institutions to disclose education records or personally identifiable information from education records if they have the written consent of the student or parent, if the disclosure meets one of the statutory exemptions or if the disclosure is directory information and the student has not placed a hold on release of directory information.

FERPA also allows the following rights:

- **The rights to inspect and review their own education records** – A written request should be made to the school and the school should offer the student or parent the right to inspect with 45 days of the receipt for access. Schools are not obliged to make copies or distribute the records unless it is impossible for the student or parent to review the records for reasons such as distance. Education institutes may charge for copies unless the fee imposed effectively prevents the student exercising his or her right to inspect and review the records. School board policy for education records should include a schedule of fees for copies that does not exceed the cost of reproduction or retrieval of the records.

- **The right to request the amendment of education records that the student believes are inaccurate, misleading, or otherwise in violation of the student’s privacy rights under FERPA** – If the school decides not to amend the record, the student or parent has the right to a formal hearing. If the school is still of the same decision, the student or
The right to provide written consent before the educational institute discloses personally identifiable information from the student’s education records - except to the extent that FERPA authorises disclosure without consent (e.g. disclosure to school officials with legitimate educational interests). The educational institution may also disclose personally identifiable information from records without consent if it relates to an emergency if the information is necessary to protect the health and safety of the student or others. Schools may also disclose, without consent, certain ‘directory’ information such as a student’s name, address, phone number, honours and dates of attendance. However the school must inform the student or parent about the directory information and give the student or parent a reasonable amount of time to request the school to not make the disclosure.

The right to file a complaint with the US Department of Education concerning alleged failures by the institution to comply with the requirements of FERPA.

The consequences of non-compliance with the FERPA requirements may include official notice from the Department of Education to cease the practice of non-compliance. The Secretary of Education may also withhold funding from the institution due to non-compliance.

**Summary**

The Family Educational Rights and Privacy Act of 1974 (FERPA) (or the Buckley Amendment) is a US Federal law that protects the privacy of student education records i.e. records, files, documents and other materials containing information directly related to a student that are maintained by an educational institution.

**CIPP Exam Preparation**

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Family Educational Rights & Privacy Act of 1974 (FERPA) (II.D.a.)
Telemarketing Regulations & Requirements

Telemarketing is a practice in which a business initiates a phone call to propose a commercial transaction. Most people are familiar with the practice, as millions of telemarketing calls are made to individuals each year. Needless to say, this is a highly unpopular practice among Americans. Public opinion surveys on the telemarketing industry reflect that the majority of Americans object to unsolicited sales calls.

In the US, telemarketing is regulated by two federal statutes:

2. Telemarketing and Consumer Fraud Abuse Prevention Act

**TEST TIP!**

**Telephone Consumer Protection Act of 1991 (TCPA)**

Under the Telephone Consumer Protect Act (TCPA), the following practices are prohibited:

- Automatic dialing systems or prerecorded voices to make sales calls to emergency phone lines, medical offices, hospital rooms, homes for the elderly, paging services or cellular phones.
- Use of artificial or prerecorded voice telemarketing, except where there is an emergency, or the recipient has given prior consent.
- Transmission of unsolicited commercial facsimile messages (i.e. “junk faxes”).

The TCPA makes the following requirements:

- All commercial facsimile messages must include accurate date, time and sending telephone number information in the margin.
- The creation of a private right of action allowing individuals, businesses, and state officials to bring a case in court for minimum damages of $500 and up to $1500 in damages, where the telemarketer “knowingly,” or “willfully” violated the TCPA.
- The opportunity for the Federal Communications Commission (FCC) to issue regulations to improve protections against telemarketing, including the ability to create a national Do-Not-Call list.
The opportunity for states to enact legislation to increase protections against the sending of junk faxes, the use of autodialing systems, the use of prerecorded and artificial voice systems and the making of telephone solicitations.

The TCPA is enforced by the FCC.

**Do-Not-Call Registry**

The national Do-Not-Call Registry gives consumers a choice about whether they want to receive telemarketing calls at home. Once individuals register their phone number, telemarketers covered by the national register have up to 31 days to stop calling the number.

The Registry is managed by the Federal Trade Commission (FTC) and is enforced by the FTC, FCC and state law enforcement officials.

**Telemarketing and Consumer Fraud Abuse Prevention Act (TCFAP Act)**

The TCFAP Act addresses specific aspects of telemarketing and permits the FTC to issue the Telemarketing Sales Rule (TSR).

The TSR imposes the following restrictions on telemarketers:

- Telemarketers must make certain disclosures at the outset of the sales call:
  - Name of the seller
  - That the call is made for sales purposes
  - Total charge of the sale
  - Any restrictions on the sale
  - If a refund policy exists
- Sweepstakes telemarketing involves special disclosures:
  - No purchase is necessary in order to participate
  - The odds for winning
  - If there is a cost associated with participation
- Calls cannot be initiated before 8AM or after 9PM in the recipient’s time zone.
- Telemarketers must obtain “express verifiable authorization” before engaging in certain transactions (e.g. making a draft directly from a bank account).
- Telemarketers must maintain records, including records of advertisements, sales records and employee records.
Note that the TSR does not apply to certain forms of telemarketing. For instance, most business-to-business sales calls; telemarketing by banks, federal financial institutions, common carriers, insurance companies and non-profit organizations are exempt from the TSR.

Summary

Telemarketing is a common practice in the US, as it is an inexpensive way to market products. However, public opinion polls reflect that it is highly unpopular among Americans. The article introduces two federal laws that regulate telemarketing: the Telephone Consumer Protection Act of 1991 (TCPA) and the Telemarketing and Consumer Fraud Abuse Prevention Act (TCFAP Act). The article also discusses the Federal Trade Commission's (FTC's) Telemarketing Sales Rules (TSRs) and the national Do-Not-Call Registry.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Telemarketing Sales Rules (TSR) and the Telephone Consumer Protection Act of 1991 (TCPA) (II.E.a.)
- Do-Not-Call Registry (DNC) (II.E.a.i.)
Email Privacy & CAN-SPAM Act

Email has become one of the most prevalently used tools in communication between commercial entities and consumers. However, the use of email for marketing has inundated users’ inboxes with unwanted messages—some legal, others not. Both consumers and businesses must understand current legislation regarding electronic marketing messages to protect personal privacy and use direct marketing effectively.

What is Spam?

Spam is the misuse of an electronic messaging system to send unsolicited marketing messages to a large numbers of recipients at one time. Spam is most commonly sent over email, but may also occur over text messages, instant messages, community forums and chat rooms. Other than being a hassle to recipients, spam may cause other problems. Some spam messages contain viruses. Spam can also overload mail servers causing service outages. Despite anti-spam laws, spam continues to remain a viable marketing method because sending indiscriminate mass mailings costs little overhead and is difficult to track.

How are Marketing Messages Different from Spam?

Not all messages advertising a product are considered spam, even if the recipient may feel they are unwanted. Marketing messages which follow a certain guidelines are a legitimate form of advertising. They improve customer loyalty and repeat business as well as attract new customers. They also alert consumers to special deals available to them and introduce them to new products and services.

Spam legislation recognizes the benefits and necessity of electronic marketing messages and has not outlawed their use, provided companies advertise honestly and give users the ability to stop receipt of marketing messages.

The CAN-SPAM Act

The Controlling the Assault on Non-Solicited Pornography and Marketing Act was passed in 2003 with the aim of reducing the amount of unsolicited marketing messages, particularly those with sexually explicit content. The CAN-SPAM Act delineates between a commercial email message which specifically advertises products or services and transactional or relational email messages which are used in the process of rendering a service.
The act allows unsolicited marketing messages to be sent as long as the sender provides an opt-out mechanism, the message contains certain identifying information (see below), and does not use harvested email addresses or an open relay to send messages. The CAN-SPAM Act has been criticized because it prevents states from implementing strong regulations and disallows customers from suing spammers.

The Elements of a CAN-SPAM Compliant Marketing Message

- The message contains an accurate and identifying header— the “From,” “To,” “Reply To,” and similar information fields must accurately identify the sender
- The message uses accurate, unambiguous subject lines— the subject line must reflect the content of the message
- The message must identify itself an advertisement somewhere within the body or header of the message.
- The message must include a valid physical address or location where the recipient may contact the sender.
- The message includes a working opt-out mechanism— requests must be honored within 10 business days

The E-Privacy Directive

The Directive on Privacy & Electronic Communications is the main spam law in the E.U. It was passed in 2002 as a supplement to the protections covered under the European Data Directive. The E-Privacy Directive deals with privacy issues on the Internet such as cookies and spam. Article 13 bans entities from sending unsolicited marketing messages unless the data subject has opted in to receiving such email. The E-Privacy Directive does not prevent the transmission of transactional messages or marketing messages advertising similar products or services.

Conclusion

Marketing messages serve an important purpose in the world of advertising and can be beneficial to both consumers and businesses, when used correctly. Though spam may never be fully eliminated, if consumers understand their personal right to privacy and businesses follow legitimate electronic marketing practices, the amount of spam reaching recipients can certainly be reduced.
CIPP Candidate Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post including:

- Combating the Assault of Non-Solicited Pornography and Marketing Act of 2003 (II.E.b.)
Junk Fax Prevention Act (JFPA)

The Junk Fax Prevention Act (JFPA) was passed by Congress in 2005 in order to maintain the “established business relationship” exception, which allows associations and companies to send unsolicited faxes to their members and clients.

What does the JFPA do?

The JFPA was passed in response to a rule developed by the Federal Communications Commission (FCC) in 2003 that would have prohibited commercial faxes sent without a recipient’s prior written consent. As the rule was to take effect July 1, 2005, Congress expedited the JFPA. The Act was further promoted by the American Society of Association Executives (ASAE) and the Fax Ban Coalition, which resulted in the FCC granting an additional six-month stay, which postponed the effective date to January 9, 2006, allowing time for the FCC to write a new rule incorporating the mandates of the legislation.

The JFPA “grandfathers” in fax numbers in the possession of the sender at the time of the enactment and brings back the “established business relationship” language that had been removed by the FCC rule. In addition, the Act stipulated that:

- All unsolicited commercial faxes must include an opt-out provision on the first page of the fax, offering a cost-free, 24-hour option for the recipient to request to be removed from the fax distribution list.
- Fax numbers be obtained directly from the recipient or from a public source to which the recipient gave the number for publication (i.e. a web site advertisement or directory)

FCC Actions

The JFPA directed the FCC to amend its rules adopted pursuant to the Telephone Consumer Protection Act (TCPA) with regards to fax advertising. The FCC’s revised rules are as follows:

1. Codify an established business relationship (EBR) exemption to the prohibition on sending unsolicited fax advertisements.
2. Define EBR for unsolicited fax advertisements.
3. Require the sender of fax advertisements to provide specified notice and contact information on the fax that allows recipients to “opt-out” of any future faxes from the sender.
4. Specify the circumstances under which a request to “opt-out” complies with the Act.
Note that the FCC rules provide the following definitions:

- **“Unsolicited advertisement”** – “Any material advertising the commercial availability or quality of any property, goods, or services which is transmitted to any person without that person’s prior express invitation or permission, in writing or otherwise."

- **“Established business relationship”** – “A prior or existing relationship formed by a voluntary two-way communication between a person or entity and a business or residential subscriber with or without an exchange of consideration [payment], on the basis of an inquiry, application, purchase or transaction by the business or residential subscriber regarding products or services offered by such person or entity, which relationship has not been previously terminated by either party.”

### Fax Numbers and the National DNC List

Registering a home phone number on the national Do-Not-Call list prevents only telephone solicitations directed to that number, not fax advertisements to individuals’ home or business fax numbers. The FCC’s junk fax rules prohibit fax advertisements, unless individuals have an EBR with the sender or have provided prior express permission to receive the fax advertisements.

The FCC has the authority to issue warning citations and impose fines against companies violating or suspected of violating the junk fax rules, but does not award individual damages. An individual who suspects that he/she has received an unauthorized fax advertisement can file a complaint with the FCC at no charge. This can be done via the online complaint form, or with the FCC’s Consumer Center.

### Responses to the JFPA

**Worldwide ERC** General Counsel Dick Mansfield commented on the JFPA, saying that:

“Because of the complexity of the legal and transactional aspects of employee mobility, many time-sensitive documents must be sent by fax. The Junk Fax Prevention Act just signed by the President removes a looming ambiguity from the law, and allows employee mobility to proceed using the most efficient tools without fear of inadvertent legal sanction.”

### Summary

The 2005 Junk Fax Prevention Act (JFPA) was passed in response to a Federal Communications Commission (FCC) rule. The Act brings back the “established business
relationship” exemption and outlines specific requirements for the sending of fax advertisements.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Junk Fax Prevention Act (II.E.c.)
The Wireless Domain Registry

The **Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003** (CAN-SPAM Act) aims to prohibit the transmission of commercial messages to any address referencing an Internet domain name associated with a wireless subscriber messaging service, unless the individual addressee has given the sender express prior authorisation to assist senders of commercial messages in identifying the addresses that belong to wireless subscribers, the Act required that wireless service providers supply the Federal Communication Commission (FCC) with the names of the relevant domain names. The object of the Act is to cut down on unwanted spam to wireless phones and other devices without the express consent of the consumer.

The FCC’s **Telephone Consumer Protection Act** (TCPA) prohibits marketers from using automatic dialling systems to make calls to wireless parties, unless it is an emergency situation or the marketers have express prior consent. Wireless devices may include cell-phones, pagers, etc.

A ‘mobile service commercial message’ (MSCM) is an e-mail message that is sent to an e-mail address on an Internet domain of a wireless carrier. Most wireless carriers maintain an Internet domain name that can be used to send MSCMs to the wireless devices of users on their network.

In 2004 the FCC announced that carriers could begin to submit their wireless domain names to the FCC for inclusion in a wireless domain names database. This list is updated regularly as the Commission receives additional submissions. Under the regulations, carriers must:

- File any future updates to listings with the Commission not less than 30 days before issuing subscribers any new or modified domain names.
- Remove any domain name that has not been issued to subscribers or is no longer in use within 6 months of placing it on the list or last date of use.

The wireless domain list was made available in 2005 and marketers are required to adjust any e-mail campaign lists accordingly. Unless a recipient has given express prior authorisation, a person must not initiate marketing via e-mail to any address with a domain name that has been on the list for at least 30 days before the message is sent or otherwise knowingly initiate a mobile service commercial message.

If prior authorisation is given, the rules provide that senders of commercial e-mails must comply with the following:

- Stop sending MSCMs within 10 days of receiving an opt-out request from a commercial wireless service provider.
- Place a ‘conspicuously marked opt-out mechanism’ in the MSCM so that consumers can request that they no longer be sent additional MSCMs.
- Provide the customers with the opportunity to opt-out via the same electronic method by which they initially provided their consent.
- Have at least one opt-out mechanism that is free of charge.
- Clearly identify to consumers who the sender is. For example, if a third party sends commercial e-mails on a company’s behalf, the e-mails must have the latter’s name clearly marked as the sender of the e-mail.
- Keep operational the opt-out mechanism identified in the MSCM for at least 30 days following the transmission of an MSCM.

The FCC list is provided by wireless carriers as opposed to individual customers. The Federal Trade Commission (FTC) has previously rejected a national do-not-spam registry due to fears that spammers would obtain the list and, as a list of working e-mail addresses, spam them.

The FTC is the primary enforcer of the CAN-SPAM Act but federal, state and private parties can also bring claims for violation. Penalties for non-compliance vary on the party bringing the claim and on whether the violation was ‘wilful, knowing of aggravated.’ Penalties may be up to $11,000 per violation.

**Summary**

As part of the federal CAN-SPAM Act, the FCC must require cell providers (i.e. commercial mobile radio services) to turn over the names of the internet domains on which they provide service. This article explores the so-called “wireless domain registry.”

**CIPP Exam Preparation**

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Wireless Domain Registry (II.E.d.)
Telecommunications Act of 1996 and Consumer Proprietary Network Information

The Telecommunications Act of 1996

The Telecommunications Act of 1996 was signed by Congress with the intention on providing customers with more competition and diversity from their telecommunication services.

Section 222(a) of the 1996 Act states: “Every telecommunication carrier has a duty to protect the confidentiality of proprietary information of and relating to customers.”

This restricts the use of Customer Proprietary Network Information (CPNI) to the limited purpose of providing the telecommunications services from which the CPNI was derived in the first place. For any other purposes the carrier must obtain consent from the customer before using or disclosing CPNI. It also limits the rights of a carrier or provider to use CPNI to gain unfair competitive advantage in relation to other carriers.

Customer Proprietary Network Information

In 1998, the Federal Communications Commission’s (FCC) interpretation of section 222 of the 1996 Act identified that customer information could potentially be used in a manner that was invasive of customer privacy and published a rules to govern the specific uses of customer information by telecommunication companies. Under the rules, all service providers and carriers have a duty to protect against the unauthorised disclosure of customers’ CPNI and must have internal safeguards in place.

Information referred to as CPNI is information that can be gathered and used by telecommunication companies for marketing purposes and includes:

- Information about the quantity, technical configuration, type, destination, location and amount of use of your communications services.
- Information contained on your bill concerning your communications services.

Examples of CPNI may include telephone numbers that the customer calls or communications services that they purchase. It does not include the customer’s name, address or telephone number or other specific identifiable information. CPNI does not include information related to the internet, which is defined as an ‘information service’.

In 2006, the FCC strengthened the protection to protect against a practice known as ‘pretexting’ i.e. posing as the actual customer or as a police official to obtain telephone calling records.
Congress passed a law making this action a crime punishable by a fine or imprisonment of up to 10 years.

**US West case**

Section 222 did not define a ‘telecommunication service’. Therefore, the FCC interpreted it to be a customer’s total combination of services obtained from any one carrier (total service approach, or TSA), allowing the use of such information for cross-promotion of services.

Section 222(c)(1) of the 1996 Act called for express customer approval requirements (an opt-in scheme) that would require customers to give affirmative consent if a carrier or provider wished to promote additional services outside of the customer’s current total-service package, using CPNI. The FCC’s interpretation was considered to be an attempt to balance the privacy interests of consumers with the deregulatory purposes of the 1996.

In their challenge to the legislation, US West argued that this interpretation went too far and restricted the right to free speech under the First Amendment as it would “seriously impair carriers’ ability to communicate valuable commercial information to their customers.” The court agreed, stating that the FCC’s argument that alternative means of communication to customers was available (such as broadcast speech) did not eliminate the fact that their interpretation restricted speech. On that basis it held that the restriction was unconstitutional and struck it down.

On that basis the updated FCC interpretation of the 1996 Act states that service providers may use customers’ CPNI without prior approval to provide customers with information about services that are within the same category as the services that they have already purchased. Service providers may also request a customer to allow the server to share CPNI with affiliates, agents or other related entities. Rather than the ‘opt-in approach’ initially adopted by the FCC, an ‘opt-out approach’ can now be applied by the carrier. This method means that a customer is deemed to have consented to the use, disclosure or access to the customer’s CPNI if the customer has failed to object to the notification of the carrier’s request for consent. However, the carrier must inform the customer of their preferred method and, if the company is using the ‘opt-out approach’ the notice must provide a reasonable time for the customer to opt-out.

**Summary**

The Telecommunications Act of 1996 was signed by Congress with the intention on providing customers with more competition and diversity from their telecommunication services. Customer Proprietary Network Information (CPNI) is information that can be gathered and used by telecommunication companies for marketing purposes.
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

Video Privacy Protection Act of 1988

The US has unusually strict privacy protections to video rental records. This can be traced back to the confirmation hearings of Supreme Court nominee Robert Bork, during which a reporter obtained copies of Bork’s video rental records. Though the rentals were innocuous, the incident frightened Congress enough to pass the 1988 Video Privacy Protection Act (VPPA), which requires written consent from consumers before video rental records could be shared.

What is the VPPA?

The Video Privacy Protection Act of 1988 (Public Law 100-618) limits the disclosure of personally identifiable information regarding video rentals. It represents one of the strongest consumer privacy protections in federal law – even stronger than those for health records under HIPAA.

The VPPA defines “personally identifiable information” as that which “identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” A “video tape service provider” is “any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale or delivery of prerecorded video cassette tapes or similar audiovisual materials.”

Video tape service providers may disclose personally identifiable information only:

- To the consumer himself/herself
- To any other person, with the written consent of the consumer
- To any other person, if this disclosure is simply of names and addresses and:
  - The consumer has been provided with an opportunity to opt-out and
  - The disclosure does not identify title, description or subject matter (though subject matter may be disclosed “for the exclusive use of marketing goods and services to the consumer”)
- To any other person, if in the ordinary course of business
- To a law enforcement agency, pursuant to a federal or state warrant, a grand jury subpoena, or a court order, provided that:
  - The consumer is provided with prior notice and
  - There is a showing of probable cause to believe that the records are relevant to a legitimate law enforcement enquiry
- Pursuant to a court order in a civil proceeding, upon showing of a compelling need, provided
  - The consumer is given reasonable notice and
  - Afforded the opportunity to contest the request
Responses to the Act

It’s important to note that the VPPA is very rarely applied; however, it represents one of the strongest protections of consumer privacy against a specific form of data collection. In general, it prevents disclosure of personally identifiable rental records of video cassette tapes or similar audio visual material, but beyond that it has several important provisions, including:

- A general ban on the disclosure of personally identifiable rental information unless the consumer consents specifically and in writing.
- Disclosure to police officers only with a valid warrant or court order.
- Disclosure of “genre preferences” along with names and addresses for marketing, but allowing customers to opt out.
- Exclusion of evidence acquired in violation of the VPPA.
- Civil remedies, including possible punitive damages and attorneys’ fees, not less than $2500.
- A requirement that video stores destroy rental records no longer than one year after an account is terminated.
- The VPPA does not preempt state law. This means that states are free to enact broader protections for individuals’ records.

Updates to allow online sharing

In December 2011, the House of Representatives passed legislation updating the VPPA in order to facilitate online rental services – such as Netflix – to share information about customers’ viewing habits with user consent. Previously, the law required written consent to share video records, however the new law allows companies to obtain consent over the web.

Specifically, it would amend the VPPA’s consent provision to allow the disclosure of video rental records:

- to any person with the informed, written consent (including through an electronic means using the Internet) in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer given at one or both of the following times –
  
  i. the time the disclosure is sought; and
  
  ii. in advance for a set period of time or until consent is withdrawn by such consumer.

The legislation was sponsored by Rep. Bob Goodlatte (R-VA) and updates the VPPA to allow users to consent to video sharing over the web. It also allows users to consent once to all future sharing. These adjustments were criticized by Marc Rotenberg, president of the Electronic Privacy Information Center (EPIC).
Summary

This article takes a look at the Video Privacy Protection Act of 1988 (VPPA), which limits the disclosure of personally identifiable information regarding video rentals. It represents one of the strongest consumer privacy protections in federal law and was passed as a response to the disclosure of Supreme Court nominee Robert Bork’s video rental records during his confirmation hearings.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Video Privacy Protection Act of 1988 (II.E.f.)
Cable Communications Privacy Act of 1984

The Cable Communications Privacy Act (Public Law 98-549) protects the personal information of customers of cable service providers. It incorporates the provisions of the OECD Privacy Guidelines (1980), thus providing a model of a comprehensive privacy statute. At the same time, it also represents an example of US sector-by-sector approach to privacy law.

What is the Cable Act?

In 1984, Congress passed the Cable Communications Privacy Act ("1984 Cable Act," or simply "Cable Act") to amend the Communications Act of 1934. The Cable Act establishes a comprehensive framework for cable regulation and puts forward strong protections for subscriber privacy by restricting the collection, maintenance and dissemination of subscriber data.

The Cable Act prohibits cable operators from using the cable system to collect "personally identifiable information" concerning any subscriber without prior consent, unless the information is necessary to render services, or detect unauthorized reception. It also prohibits operators from disclosing personally identifiable data to third parties without consent, unless the disclosure is either necessary to render a service provided by the cable operator to the subscriber or if it is made to a government entity pursuant to a court order.

Under the Cable Act, cable companies are required to provide a written notice of privacy practices to each subscriber/customer at the time of entering into a service contract, and at least once a year thereafter. The privacy notice must specify:

- The nature of the personally identifiable information that is or may be collected, and the uses to which it may be put.
- The "nature, frequency and purpose" of any disclosure that may be made of such information, including identification of the persons to whom those disclosures may be made.
- How long the information may be maintained by the cable service provider.
- Where and how the subscriber may have access to the information about himself/herself.
- The subscriber’s right to bring legal action if the requirements of the law are not followed.
Consent, Disclosure & Access

Generally, cable service providers are required to obtain prior written or electronic consent from their customers before the collection of personal information. Consent is not required to obtain information “necessary to render cable services,” nor is it required for information used to detect unauthorized reception.

Under the Cable Act, disclosure requires prior consent, with the same two exceptions for business necessity and detection of cable piracy. Disclosure of personal information without consent is also permitted pursuant to a court order. The subscriber must be first notified, and presented with an opportunity to appear and contest the order. Generally, disclosures may not include information about the subscriber’s particular selections of video programming.

Cable service customers must be offered access to the personal information collected “at reasonable times and at a convenient place.” The customer must be provided with a reasonable opportunity to have any errors in that information corrected. It is also the responsibility of the service provider to destroy personal information when it is no longer needed for the purposes for which it was collected. The company must take appropriate steps to prevent unauthorized access of customers’ personal information for as long as it is held.

Cable service subscribers have rights for civil action in cases of violation of the Cable Act. The Act includes provisions for actual and punitive damages.

Updates to the Act

In 2001, the USA-PATRIOT Act narrowed the Cable Act’s privacy provisions, clarifying that companies who offer cable-based internet or telephone services will be subject to the requirements of the Cable Act to notify subscribers of government surveillance requests only when detailed cable viewing information is being sought. Otherwise, cable operators can respond to a government surveillance request under the Electronic Communications Privacy Act (ECPA), which does not require service providers to notify subscribers of requests.

Summary

This article introduces the Cable Communications Privacy Act of 1984 (CCPA, or “Cable Act”), which protects the personal information of customers of cable service providers.
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Cable Communications Privacy Act of 1984 (II.E.g.)
End-of-Chapter Review

Federal Trade Commission Act (FTC Act)

- Establishes the FTC, tasked with investigating businesses for evidence of UDTP
- “Antitrust” legislation
- FTC to have five members, seven-year terms
- Permits FTC to issue “cease and desist” orders to large corporations for UDTPs

Children’s Online Privacy Protection Act of 1998 (COPPA)

<table>
<thead>
<tr>
<th>Who is covered?</th>
<th>Commercial website operators.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is covered?</td>
<td>Collection and use of information collected through a commercial website from children under 13 years old.</td>
</tr>
<tr>
<td>What is required or prohibited?</td>
<td>Website operators need verifiable parental consent before collecting personal information from children.</td>
</tr>
</tbody>
</table>
| Who enforces the law? | • FTC  
• State Attorneys General |
| What happens if there is no compliance? | • Lawsuits  
• Reputation damage |
| Why does the law exist? | To respond to websites collecting personal information from young children. |
### Health Insurance Portability and Accountability Act of 1996 (HIPAA)

| Who is covered? | **Directly**: Health care providers, health plans, health care clearinghouses  
<table>
<thead>
<tr>
<th></th>
<th><strong>Indirectly</strong>: Business associates, those who use/disclose PHI (personal health information). These are covered contractually.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is covered?</td>
<td>PHI transmitted or maintained in any form.</td>
</tr>
</tbody>
</table>
| What is required or prohibited? | Covered entities may not use/disclose PHI except as permitted/required by HIPAA.  
|                             | Permitted uses include:  
|                             | - For treatment, payment, operations (TPO)  
|                             | - With informal consent, in the individual’s best interests  
|                             | - For public health purposes  
|                             | - Incidental uses/disclosures  
|                             | - With the individual’s written authorization  
|                             | Required uses include:  
|                             | - To the individual, upon request  
|                             | - To HHS, for compliance |
| Who enforces the law? | - Department of Health & Human Services  
|                         | - Office of Civil Rights (Privacy Rule)  
|                         | - Centers for Medicare & Medicaid Services (Security Rule)  
|                         | - State Attorneys General |
| What happens if there is no compliance? | Civil and criminal penalties; fines up to $250,000; and/or 10 years imprisonment. |
| Why does the law exist? | - Provides the basis for medical privacy; HIPAA does not preempt state laws.  
|                         | - Facilitate the move towards electronic medical records. |

### HIPAA Privacy Rule

- Privacy official must be appointed.  
- Use/disclosure of data must be limited to the minimum necessary.  
- Privacy notices must be delivered with mandated content.  
- Disclosures must be recorded.  
- Individual requests regarding PHI disclosures and communications must be respected.  
- Complaints process must be established.  
- Appropriate security must be ensured.  
- Psychotherapy notes must follow special rules.
### HIPAA Security Rule

- Applies to electronic PHI (EPIH).
- Requires reasonable security.
- Provides comprehensive security requirements with implementation specifications.
- Entities must assess if addressable specifications are required.

### Health Information Technology for Economic & Clinical Health Act (HITECH Act)

| Who is covered? | **Directly:** Health care providers, health plans, health care clearinghouses  
**Indirectly:** Business associates, those who use/disclose PHI (personal health information). |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| What is covered?| Adjusted the HIPAA of 1996, creating new requirements concerning privacy and security for health information that may (materially and directly) affect more entities, businesses and individuals.  
Covered entities may not use/disclose PHI except as permitted/required by HITECH.  
“Business associates” = persons and organizations that perform activities which involve the use/disclosure of personally identifiable health information. Includes organizations that transmit PHI and those that require access on a routine basis. |
| What is required or prohibited? | New security breach notice requirements.  
Individuals entitled to electronic copies of their health information from any health plan or health care provider that uses/maintains EHRs. |
| Who enforces the law? |  
- Department of Health & Human Services  
- Office of Civil Rights (Privacy Rule)  
- Centers for Medicare & Medicaid Services (Security Rule)  
- State Attorneys General |
| What happens if there is no compliance? | Civil and criminal penalties; fines up to $250,000; and/or 10 years imprisonment. |
| Why does the law exist? | Adjusts the HIPAA with more stringent requirements, particularly regarding breach notification. |
### Fair Credit Reporting Act

| Who is covered? | • Persons that compile consumer reports (i.e. consumer reporting agencies (CRAs))  
|                | • Persons who use consumer reports |
| What is covered? | Consumer reports |
| What is required or prohibited? | • Third party data must be accurate, current and complete.  
|                            | • Notice must be provided to consumers when third party data is used to make adverse decisions about them.  
|                            | • Consumer reports may only be used for permissible purposes.  
|                            | • Consumers must be able to access and correct errors on consumer reports.  
|                            | • Must comply with other requirements on users and furnishers of consumer information. |
| Who enforces the law? | • FTC  
|                        | • State Attorneys General  
|                        | • Private right of action |
| What happens if there is no compliance? | • Civil and criminal penalties  
|                       | • $1000/violation; $2500/willful violations |
| Why does the law exist? | • Enacted in 1970; first national privacy law in the world  
|                        | • To mandate reasonable accuracy, access and correction to consumer reports  
|                        | • Limit use of consumer reports  
|                        | • 1996: amendment to allow financial institutions for pre-screening  
|                        | • 2003: amendment with provisions regarding identity theft (FACTA – Fair & Accurate Credit Transaction Act) |
# Fair and Accurate Credit Transactions Act of 2003 (FACTA)

<table>
<thead>
<tr>
<th>Who is covered?</th>
<th>Any person or company that maintains and retains consumer information for a business purpose.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is covered?</td>
<td>Consumer reports</td>
</tr>
<tr>
<td>What is required or prohibited?</td>
<td>Assistance with identity theft: free credit reports; fraud alerts; PAN truncation; access to information; collection agencies; red flags. Rule regarding proper disposal of consumer report information and records. Sets standards for “employee misconduct investigations.”</td>
</tr>
<tr>
<td>Who enforces the law?</td>
<td>FTC</td>
</tr>
</tbody>
</table>
| What happens if there is no compliance? | Civil liability:  
  - Actual damages sustained if identity is stolen as a result of corporate inaction  
  - Statutory damages of up to $1,000/employee  
  
  Class-action lawsuits:  
  - If large numbers of employees are affected, they may be able to bring class-action suits and receive punitive damages from employers.  
  
  Federal fines:  
  - Up to $2,500/violation  
  
  State fines:  
  - Up to $1,000/violation  

| Why does the law exist? | Amends the FCRA  
  - Helps prevent ID theft  
  - Improve resolution of consumer disputes  
  - Increase accuracy of consumer records  
  - Make improvements in use of, and consumer access to, credit information |
### Gramm-Leach-Bliley Act (GLBA); Financial Services Modernization Act of 1999

| Who is covered? | Domestic financial institutions (FIs)  
|----------------|----------------------------------------  
| E.g.           | Banks, auto dealers, financial data processors, entities that educate/place financial professionals, tax lawyers, real estate lawyers.  

| What is covered? | Non-public personal financial information  
|------------------|---------------------------------------------  
| I.e.             |  
|                  | • Information provided by a consumer to a FI to obtain a product/service, or  
|                  | • Information resulting from a transaction involving a product/service between a FI and consumer, or  
|                  | • Information obtained by an FI through providing a consumer with a product/service.  

<table>
<thead>
<tr>
<th>What is required or prohibited?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• FIs must provide consumer customers with privacy and security notices.</td>
</tr>
<tr>
<td>• FIs may share any information with affiliated companies, service providers, or joint marketing partners.</td>
</tr>
<tr>
<td>• FIs may share information with non-affiliated companies, if consumers have not opted-out.</td>
</tr>
<tr>
<td>• FTC and financial institution regulators to publish privacy and safeguard regulations.</td>
</tr>
<tr>
<td>• GLBA does not preempt state laws; it represents the baseline.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who enforces the law?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• FTC</td>
</tr>
<tr>
<td>• Financial institution regulators</td>
</tr>
<tr>
<td>• State Attorneys General</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What happens if there is no compliance?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enforcement actions</td>
</tr>
<tr>
<td>• Private lawsuits</td>
</tr>
</tbody>
</table>

| Why does the law exist? | To address privacy and security of financial information (Title V).  

---

**GLBA Privacy Rule**

- Published by the FTC and federal financial regulators.
- Standards for privacy notices:
  - Consumers require initial and annual privacy notices
  - Nine categories of information
  - Opt-outs must be processed within 30 days
GLBA Safeguards Rule

Requires reasonable security, under three elements:

1. **Administrative Security**
   - Workforce risks
   - Employee training
   - Vendor Risks
2. **Technical Security**
   - Access controls
   - Encryption, where appropriate
3. **Physical Security**
   - Facilities controls
   - Business continuity
   - Disaster recovery

FTC Red Flags Rule

- To spot warning signs of ID theft and limit damage done
- Requires businesses and organizations to implement a formal Identity Theft Prevention Program
- Red flags = suspicious patterns/practices, or specific activities that indicate possibility of ID theft

Dodd-Frank Act

- Goal: improve accountability and transparency in financial system; protect US taxpayers by ending bailing; protect consumers from UDTP.
- Created Bureau of Consumer Financial Protection (BCFP), Financial Stability Oversight Council (FSOC), Federal Insurance Office (FIO), Office of Financial Research (OFR)
- Increase authority of: US Department of Treasury, Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board
- Volcker Rule
- Collins Amendment
# Family Educational Rights and Privacy Act 1974 (FERPA)

<table>
<thead>
<tr>
<th>Who is covered?</th>
<th>All schools that receive funds under an applicable program of the US Department of Education. Excludes most private and parochial schools, as they do not receive such funds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is covered?</td>
<td>Student education records (e.g. transcripts, class schedules, class rolls, academic history reports)</td>
</tr>
</tbody>
</table>
| What is required or prohibited? | Allows educational institutions to disclose education records or PII from education records if they have the written consent of the student or parent. Protects the following rights:  
  - Right to inspect and review education records  
  - Right to request amendment of education records that are believed to be inaccurate, misleading, or otherwise in violation of privacy rights under the FERPA  
  - Right to provide written consent before the institution discloses PII from the student’s education records  
  - Right to file a complaint with the US Department of Education regarding failures to comply |
| Who enforces the law? | Department of Education |
| What happens if there is no compliance? | Official notice from Dept. of Education to cease practice of non-compliance  
Secretary of Education may also withhold funding for non-compliance |
| Why does the law exist? | Protects privacy of student education records |
### Telephone Consumer Protection Act 1991 (TCPA)

<table>
<thead>
<tr>
<th>Who is covered?</th>
<th>Telemarketers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is covered?</td>
<td>Telemarketing communications</td>
</tr>
</tbody>
</table>
| What is required or prohibited? | Commercial fax messages must include accurate date, time and sending telephone number information.  
Creates private right of action.  
FCC’s powers to issue regulations broadened.  
Allows states to enact/increase protections against junk faxes, auto-dialers, prerecorded/artificial voice systems, telephone solicitations. |
| Who enforces the law? | FCC |
| What happens if there is no compliance? | Fines (between $500/call to $1,500/call)  
Class-action lawsuits |
| Why does the law exist? | Protect American public from UDTPs, telemarketing activities. |

### Do-Not-Call Registry (DNC)
- Managed by FTC
- Enforced by FTC, FCC, state law enforcement officials
<table>
<thead>
<tr>
<th>Who is covered?</th>
<th>Telemarketers</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is covered?</td>
<td>Telemarketing communications</td>
</tr>
</tbody>
</table>
| What is required or prohibited? | Certain disclosures at the outset of sales call.  
No calls before 8AM or after 9PM in recipient’s time zone.  
Must obtain “express verifiable authorization” before engaging in certain transactions.  
Must maintain records (i.e. records of ads, sales records and employee records) |
| Who enforces the law? | FTC, state attorneys general |
| What happens if there is no compliance? | Addresses specific aspects of telemarketing and permits FTC to issue the Telemarketing Sales Rule (TSR) |
### Telemarketing Sales Rules (TSR)

<table>
<thead>
<tr>
<th>Who is covered?</th>
<th>Telemarketers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is covered?</td>
<td>Telemarketing communications</td>
</tr>
<tr>
<td>TSR does not apply to:</td>
<td></td>
</tr>
<tr>
<td>- Non-profit organizations calling on their own behalf</td>
<td></td>
</tr>
<tr>
<td>- Existing business relationships (i.e. calls to existing customers, prospects)</td>
<td></td>
</tr>
<tr>
<td>- Inbound calls</td>
<td></td>
</tr>
<tr>
<td>- Business-to-business calls</td>
<td></td>
</tr>
<tr>
<td>- Companies not subject to FTC jurisdiction</td>
<td></td>
</tr>
<tr>
<td>What is required or prohibited?</td>
<td></td>
</tr>
<tr>
<td>- Numbers must be screened against the Federal Do-Not-Call Registry</td>
<td></td>
</tr>
<tr>
<td>- Rules for automated dialers</td>
<td></td>
</tr>
<tr>
<td>- Calls can be made only between 8AM-9PM</td>
<td></td>
</tr>
<tr>
<td>- Requests not to be called back must be respected</td>
<td></td>
</tr>
<tr>
<td>- Records must be retained for 24 months</td>
<td></td>
</tr>
<tr>
<td>- All material terms must be disclosed</td>
<td></td>
</tr>
<tr>
<td>Who enforces the law?</td>
<td>FTC and FCC</td>
</tr>
<tr>
<td>What happens if there is no compliance?</td>
<td>Fines imposed by FTC and FCC.</td>
</tr>
<tr>
<td>Why does the law exist?</td>
<td>Does not preempt state laws regarding telemarketing.</td>
</tr>
</tbody>
</table>
## Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)

<table>
<thead>
<tr>
<th>Who is covered?</th>
<th>Entities who advertise products/services through email to/from the US.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is covered?</td>
<td>Transmission of commercial email messages.</td>
</tr>
</tbody>
</table>
| What is required or prohibited? | CAN-SPAM prohibits:  
- False/deceptive messages and headers  
CAN-SPAM requires:  
- Working return email address  
- Physical address  
- Identification as commercial message  
- Clear and conspicuous opt-out  
- Opt-outs processed within 10 days  
- Following of additional FTC and FCC rules |
| Who enforces the law? | FCC and FTC |
| What happens if there is no compliance? |  
- Enforcement actions  
- Fines and civil penalties |
| Why does the law exist? | To prevent unwanted electronic marketing messages. |
### Junk Fax Prevention Act (JFPA)

<table>
<thead>
<tr>
<th>Who is covered?</th>
<th>Commercial organizations sending marketing faxes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is covered?</td>
<td>Commercial faxes</td>
</tr>
</tbody>
</table>
| What is required or prohibited? | - Consent required before sending commercial faxes.  
- Faxing permitted if there is an existing business relationship (EBR) and fax number provided before sending commercial faxes.  
- EBR does not include affiliates.  
- Opt-outs must be received 24/7, processed within 30 days. |
| Who enforces the law? | FCC |
| What happens if there is no compliance? | - Lawsuits (up to $500/page)  
- Enforcement actions |
| Why does the law exist? | Prevention of junk faxes. |

### Video Privacy Protection Act of 1988 (VPPA)

<table>
<thead>
<tr>
<th>Who is covered?</th>
<th>Video tape service providers, online rental services</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is covered?</td>
<td>PII regarding video rentals</td>
</tr>
<tr>
<td>What is required or prohibited?</td>
<td>Written consent from consumers before video rental records can be shared.</td>
</tr>
<tr>
<td>Who enforces the law?</td>
<td>Law enforcement officials</td>
</tr>
</tbody>
</table>
| What happens if there is no compliance? | Civil action:  
- Actual damages of up to $2,500  
- Punitive damages  
- Attorney’s fees and other litigation costs |
| Why does the law exist? | Limits disclosure of PII regarding video rentals.  
Represents one of the strongest consumer privacy protections in federal law. |
## Cable Communications Privacy Act 1984

<table>
<thead>
<tr>
<th>Who is covered?</th>
<th>Cable operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is covered?</td>
<td>PII from cable service subscribers</td>
</tr>
<tr>
<td>What is required or prohibited?</td>
<td>Cable companies must provide a written notice of privacy practices to each subscriber/customer on an annual basis.</td>
</tr>
<tr>
<td></td>
<td>No collection of PII without prior consent.</td>
</tr>
<tr>
<td></td>
<td>No disclosure of PII to third parties without consent.</td>
</tr>
<tr>
<td>Who enforces the law?</td>
<td>Law enforcement officials</td>
</tr>
<tr>
<td>What happens if there is no compliance?</td>
<td>Civil damages, criminal penalties</td>
</tr>
<tr>
<td>Why does the law exist?</td>
<td>Protects personal information of customers of cable service providers</td>
</tr>
</tbody>
</table>
Access to Financial Data

Privacy rights proponents often find themselves at odds with policymakers developing security regulations. In order for effective monitoring to take place, the Government and law enforcement agencies require access to sensitive information about individuals including their financial transactions, and electronic and phone communications. The following laws are known colloquially as “anti-privacy laws” because they take away some individual privacy rights in the interest of trying to detect and prevent fraud, terrorism and other significant crimes.

Right to Financial Privacy Act of 1978

The Right to Financial Privacy Act (RFPA) was passed by Congress in response to the 1976 Supreme Court ruling United States v. Miller in which the court held that bank customers have no legal expectation of privacy. Under the ruling, the Federal Government could request individual financial records without restriction.

The Right to Financial Privacy Act attempted to reassert individual rights by requiring:

- Customers to receive notice of the disclosure to the government prior to the release of their records
- The creation of a mechanism for customers to challenge the disclosure of their information.
- Government agencies to keep an audit trail of all disclosures of customer information to the agency and any interagency transfers.
In order for a government agency to obtain customer financial records, they must meet one of the following requirements:

- Receive customer consent for their release
- Provide an administrative subpoena or summons
- Provide a search warrant
- Provide a judicial subpoena
- Provide an appropriate written authorization from a government agency

It is important to note that the act only applies to disclosures to the Federal Government. It does not pertain to state and local governments. While the Right to Financial Privacy Act was designed to protect customer financial privacy, it is considered an “anti-privacy law” because its protections are weaker than those granted under the fourth amendment. The US Patriot Act further weakened the law’s protection by allowing disclosure when terrorism is suspected.

**Bank Secrecy Act**

The Bank Secrecy Act (BSA), also known as the Currency and Foreign Transaction Reporting Act was passed in 1970 to help the United States Government monitor and prevent possible money laundering schemes. Under the BSA, all financial institutions must keep records about customer transactions and submit reports to the Federal Government for certain types of transactions

A **Currency Transaction Report (CTR)** must be filed for:

- Any cash financial transactions (deposit/withdrawal/exchange) made by an individual in an amount greater than $10,000
- Any cash transactions made by or for one individual in a single business day in which the aggregate total is greater than $10,000

A **Currency and Monetary Instrument Report (CMIR)** must be filed for:

- Any person or entity that transports an individual or aggregate amount greater than $10,000 into or outside of the United States in the form of currency, traveler’s checks, bank notes or other monetary instruments.

A **Suspicious Activity Report (SAR)** must be filed for:

- Abuse by an employee of the financial institution
- Violations in which a suspect can be identified and the aggregate amount is $5,000 or more.
• Violations in which no suspect can be identified and the aggregate amount is $25,000 or more.
• A transaction through a bank in which the teller has reason to believe may be designed to avoid BSA regulations
• A transaction through a bank in which the teller has reason to believe may involve potential money laundering or criminal activity

Many banks use automated records systems that keep customer information on file and generate the relevant reports when such transactions occur. The creation of multiple reports for a single person or entity signals law enforcement agencies to look closer for fraudulent activity.

Summary

This article introduces two “anti-privacy” laws: the Bank Secrecy Act (BSA) and the Right to Financial Privacy Act (RFPA).

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

• Access to financial data (III.A.a.)
• Right to Financial Privacy Act of 1978 (III.A.a.i.)
• Bank Secrecy Act (III.A.a.ii.)
The Electronic Communications Privacy Act (ECPA) and the Stored Wire Electronic Communications Act (SWECA) are often combined and referred to as the Electronic Communications Privacy Act of 1986. The ECPA updated the Federal Wiretap Act of 1968, which was written in the context of interception of conversations using “hard” telephone lines. The update was necessary to keep up with the development of computer and other digital and electronic communications. The USA-PATRIOT Act and other federal enactments have since clarified and updated the ECPA, introducing less stringent restrictions on law enforcement access to stored communications in certain cases.

What is the ECPA?

The Electronic Communications Privacy Act (ECPA) consists of three parts:

- **Title III** – Outlaws the unauthorized interception of wire, oral, or electronic communications. Establishes a judicial supervised procedure to permit such interceptions for law enforcement purposes.
- **Stored Communications Act** – Focuses on the privacy of, and government access to, stored electronic communications.
- **Additional provisions** – Creates a procedure for governmental installation and use of pen registers, as well as trap-and-trace devices. Outlaws such installation or use, except for law enforcement and foreign intelligence investigations.

The following sections of this article explore the ECPA in greater detail.

**Title III: Prohibitions**

This section states that it is a federal crime to engage in wiretapping or electronic eavesdropping; to possess wiretapping or electronic eavesdropping equipment; to use or disclose information obtained through illegal wiretapping or electronic eavesdropping; or to disclose information secured through court-ordered wiretapping or electronic eavesdropping, in order to obstruct justice.

This prohibition applies to “any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.”

Interception, use or disclosure in violation of Title III is generally punishable by imprisonment for not more than five years and/or a fine of not more than $250,000 for individuals and not more than $500,000 for organizations.
Stored Communications Act (SCA)

The SCA bans surreptitious access to communications at rest, although it does so beyond the confines which apply to interception. The SCA includes two sets of proscriptions: a general prohibition and a second applicable only to certain communications providers.

Breaches of the unauthorized access prohibitions expose offenders to potential criminal, civil and administrative sanctions. Violations committed for malicious, mercenary, tortious or criminal purposes are punishable by imprisonment for not more than five years, and/or a fine of not more than $250,000.

Pen Registers & Trap-and-Trace Devices

A trap-and-trace device identifies the source of incoming calls, while a pen register indicates the numbers called from a particular instrument. They do not allow users to overhear the contents of a phone conversation or to otherwise capture the content of a communication and were not considered interceptions under Title III prior to the enactment of the ECPA.

Title III wiretap provisions apply when pen registers and trap-and-trace devices are able to capture wire communication content. The USA-PATRIOT Act enlarged the coverage to include sender/addressee information relating to email and other forms of electronic communications.

Federal government attorneys and state and local police officers may apply for a court order authorizing the installation and use of a pen register and/or a trap-and-trace device upon certification that the information it will provide is relevant to a pending criminal investigation.

The use or installation of pen registers or trap-and-trace devices by anyone other than the telephone company, service provider, or those acting under judicial authority is a federal crime, punishable by imprisonment for not more than a year and/or a fine of not more than $100,000 (or $200,000 for an organization).

Adjustments to the ECPA

Over the years, Congress has adjusted the components of ECPA and FISA. It has done so sometimes in the interests of greater privacy, sometimes in the interest of more effective law enforcement or foreign intelligence gathering, often with the objective of combining those interests.
Some important enactments include:

- The USA-PATRIOT Act
- The Intelligence Authorization Act for Fiscal Year 2002
- The 21st Century Department of Justice Appropriations Authorization Act
- The Department of Homeland Security Act
- The USA-PATRIOT Improvement and Reauthorization Act
- The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (or 2008 FISA Amendments Act)

Summary

This article takes a closer look at the Electronic Communications Privacy Act of 1986, which consists of three main parts: 1) Title III; 2) the Stored Communications Act; and 3) Additional provisions regarding pen registers and trap-and-trace devices.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Electronic Communications Privacy Act of 1986 (III.A.b.ii.)
- Emails, stored records and pen registers (III.A.b.ii.1. – III.A.b.ii.3.)
Communications Assistance for Law Enforcement Act (CALEA)

Since its enactment in 1994, privacy rights experts and watchdogs have been wary of the Communications Assistance for Law Enforcement Act (CALEA). This article explores the history of the CALEA, how it has evolved over the years and some privacy issues surrounding wiretapping and other forms of surveillance.

Background

CALEA was passed in 1994 in order to facilitate law enforcement authorities’ wiretapping of digital telephone networks. It was the first piece of legislation in history that required telecommunications companies to modify their equipment in order to facilitate government surveillance. The FBI originally proposed the CALEA in 1992. This proposal was broadly inclusive – for instance, computer networks would have been part of this Act, in the name of government surveillance.

The CALEA essentially forced telephone companies to redesign their architectures in order to facilitate wiretapping. Notably, the CALEA did not regulate data traveling over the internet.

According to privacy watchdogs, wiretapping of suspected criminal activity by law enforcement agencies can rapidly degenerate into suspicionless monitoring of the general public, which violates the Fourth Amendment.

According to the Privacy Rights Clearinghouse,

“Wiretapping is any interception of a telephone transmission by accessing the telephone signal itself.” Another related concept is ‘electronic eavesdropping,’ which is defined as “the use of an electronic transmitting or recording device to monitor conversations without the consent of the parties.”

Under US law, there are very few situations in which wiretaps are legal. However, technological improvements have made it increasingly easier to illegally wiretap communications.

Evolution of CALEA

In August 2004, the Federal Communications Commission (FCC) released a Notice of Proposed Rule Making (NPRM), which expanded the boundaries of CALEA by redefining what constitutes telephone service, concluding that broadband Internet access providers and managed VoIP systems substantially replace local exchanges and therefore are subject to the requirements of CALEA.
In August 2005, the FCC announced a Final Rule, which expanded CALEA to Internet broadband providers and certain VoIP providers.

Critics Say…

In response to the expanding reach of CALEA, the Electronic Frontier Foundation (EFF) has listed a number of objections and concerns. These are briefly summarized below.

- **Wiretapping Convenience** – According to the EFF, wiretapping is already a relatively easy practice as is. Existing legislation already permits law enforcement agencies to place Internet users under surveillance, regardless of what programs or protocols being used to communicate. The reality is that most types of surveillance has gotten easier in this day and age.

- **“Tappability Principle” is Problematic** – The FBI suggested that if something is legally searchable sometimes, it should be physically searchable all the time (the “tappability principle”). However, this could lead to all individual phones having built-in bugs, leaving consumers to trust that the phone companies or law enforcement would not activate those bugs without a legitimate reason.

- **Increased Costs for Services** – Expanding CALEA in the manner suggested by the FCC’s NPRM would cause broadband providers to spend millions of dollars restructuring their network architectures and design and manufacture surveillance-friendly technologies. This would cause telecommunications bills to skyrocket. It would also eliminate privacy-friendly technologies from the marketplace.

- **Takes a Toll on Innovation** – CALEA compliance would significantly reduce the scope of technological research and development. It would also allow the FCC to have authority over a wider range of technologies. CALEA’s requirements might result in economic incentives for software developers to create new programs (e.g. email, IM programs) that are more surveillance-friendly. This would mean that innovators will need to work within the guidelines of CALEA’s surveillance.

- **Phone Regulations are not Applicable** – The NPRM assumes that regulations that apply within the phone network (a closed, insulated system) should be extended to the internet (an open, always-changing system). This could severely hamper technological development and innovation on the Internet, where new services and devices are being introduced all the time.

- **Internet Insecurities** – Unfortunately, many of the technologies that are used to create surveillance-friendly computer networks might increase the risk of attacks or breaches of personal data. Broadband service providers who must make their networks or applications more tappable end up introducing potential points of vulnerability into their system. Many users are unaware of this reality when they register for such services.
Surveillance-Industrial Complex

Services that facilitate wiretapping, and the types of policies that are necessitated by such legislation as the CALEA essentially facilitates what the American Civil Liberties Union (ACLU) refers to as the surveillance-industrial complex, which involves the integration of private individuals and organizations with a government-sanctioned surveillance network. Private entities motivated by profiting from surveillance activities have an incentive to lobby for increased government surveillance authority.

Regarding the CALEA, the ACLU comments,

“Americans have long feared the specter of the government maintaining dossiers filled with information about the lives of individual, innocent citizens. Data retention, whether mandatory or de facto, achieves the same goal indirectly, by ensuring that information is stored by corporations – from where, as we have seen, it can easily be accessed by the authorities.”

Summary

This article takes a look at the Communications Assistance for Law Enforcement Act (CALEA), which was passed in 1994 to facilitate law enforcement authorities’ wiretapping of digital telephone networks. In 2004, the FCC suggested substantial expansions in the scope of the CALEA in its Notice of Proposed Rulemaking (NPRM). In August 2005, the FCC’s Final Rule expanded the CALEA to include Internet broadband and VoIP providers. This article also explores privacy watchdogs’ criticism of government surveillance expansion.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Communications Assistance to Law Enforcement Act (III.A.c.)
Foreign Intelligence Surveillance Act of 1978

During the 1970s it was revealed that the US government had engaged in a huge amount of unauthorized spying during the 1960s and early 1970s. For this reason, Congress decided to provide a legal framework to curb foreign intelligence investigations. The Foreign Intelligence Surveillance Act of 1978 (FISA), along with other amendments to the Act, created a warrant procedure for foreign intelligence investigations, so that there would no longer be any foreign intelligence surveillance without court oversight.

What is the FISA?

Signed into law in 1978, the FISA requires the government to obtain search warrants and wiretap orders from a court even when it is investigating foreign threats to national security.

All government requests for foreign intelligence surveillance authorization are made to the FISA court, which many argue function as a secret court. In order to qualify for authorization, a significant purpose of the surveillance must be to gather foreign intelligence information – information about foreign spies, foreign terrorists and other foreign threats – rather than providing evidence of a crime.

In the FISA court, the probable cause standard is quite different. Instead of having to show probable cause that a crime is being, has been, or will be committed, the government must show that the target of the surveillance is a foreign power or an agent of a foreign power.

Unlike law enforcement surveillance, the target is never told by the government that he/she was spied on, and every person served with a FISA search warrant, wiretap or pen/trap order, or subpoena is also served with a gag order forbidding them from telling anyone about it, other than their lawyer.
What is a “foreign power”?

When it comes to FISA surveillance, it’s unclear exactly what qualifies as a foreign power or an agent of a foreign power. The FISA law defines those terms vaguely. Without access to the decisions of the secret FISA court, there’s no way to be sure how broadly or narrowly the definitions are being interpreted.

Under FISA, a foreign power includes:

- Any foreign government or component of a foreign government, whether or not officially recognized by the US.
- Any “faction” of a foreign nation(s). Any foreign-based political organization that isn’t “substantially” composed of US persons. Note that under the FISA, “faction” and “substantially” aren’t clearly defined, while a “US person” is considered a citizen or legal resident of the US.
- Any entity, such as a political organization or a business, that is directed or controlled by a foreign government.
- Any group engaged in, or preparing to engage in “international terrorism.” This term is broadly defined as activities that:
  - Involve violent acts or acts dangerous to human life that are a violation of US criminal laws or would be a violation if committed in the US.
  - Appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by assassination or kidnapping.
  - Occur totally outside the US, or transcend national boundaries in terms of how they are accomplished, the people they are intended to coerce or intimidate, or the place where the terrorists operate.

FISA Wiretaps

It’s important to note that FISA surveillance is quite rare, though when it takes place it includes the communications of many individuals. As information released regarding FISA surveillance is so limited, it is difficult to determine just how many people are affected and how many communications are intercepted.

The only FISA data available to the public are the numbers of applications made to, and approved by, the FISA court. Currently, FISA orders outnumber all federal and state wiretap orders combined.
FISA extension

In September 2012, the House of Representatives voted to reauthorize the 2008 amendments to the FISA (Foreign Intelligence Surveillance Act’s Amendments Act of 2008). This was a controversial piece of legislation challenged by privacy advocates and civil liberties organizations nationwide.

Under the Amendments Act, the government was permitted to conduct widespread and blanketing snooping of emails and phone calls of US persons. Section 702 of the FISA Amendments specify that the government can eavesdrop on emails and phone calls sent from US citizens to persons reasonably suspected to be located abroad without ever requiring intelligence officials to obtain a court order.

Summary

Signed into law in 1978, the Foreign Intelligence Surveillance Act (FISA) requires the government to obtain search warrants and wiretap orders from a court even when it is investigating foreign threats to national security.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Foreign Intelligence Surveillance Act of 1978 (III.B.a.)
USA-PATRIOT Act

The **Uniting and Strengthening of America by Providing the Appropriate Tolls Required to Intercept and Obstruct Terrorism Act** (USA-PATRIOT Act) was passed in 2001 after the September 11th terrorist attacks. The Patriot Act introduced wide changes across several sectors and amended several laws already in effect. Due to its strong focus on security, the US Patriot Act has been criticized for the limits it places on personal privacy.

The Patriot Act introduced the following changes to privacy laws:

- Expanded the type of information the U.S. may receive by subpoenaing Internet Service Providers to include not only personally identifiable information but also session durations and times, services used, IP addresses and payment information. Disclosure may also take place if the service provider suspects danger to “life and limb”
- Title II expanded surveillance procedures:
  - Allows “Sneak and Peek” warrants to allow delayed notice of search warrants
  - Roving wiretaps that do not require the specification of carrier or third parties
  - Amended the Foreign Intelligence Surveillance Act by expanding the duration of search and surveillance orders and removing the requirement to prove reasonable cause to monitor non U.S. citizens.
  - Expanded wiretapping capabilities under the Electronic Communications Privacy Act to allow surveillance of packet switched networks.
- Allows the U.S. Government to obtain any “books, records, papers, documents and other items” that may aid in investigations to protect against terrorism.

Many Title II regulations were set to expire on Dec. 31, 2005 but were reauthorized until December 31, 2009. The USA Patriot Extension Act of 2009 seeks to extend those regulations even further.

**Title III attempts to prevent money laundering to deter terrorism by amending the Bank Security Act and the Money Laundering Control Act of 1986.**

Subtitle I placed strong regulations on financial institutions, especially with regard to transactions with foreign countries. It expanded record keeping requirements, prohibited transactions with banks not subject to a banking authority and expanded the definition of money laundering.

Subtitle II allows suspicious activity reports to be sent to U.S. Intelligence agencies and made it illegal to structure transactions in such a way as to avoid BSA regulations.

Subtitle III made the evasion of currency reporting a criminal offense. It also made further provisions to deter money laundering.
The Patriot Act contained several other regulations that affected immigration law, criminal law, created funding for necessary defenses and provided funds for victims of terrorist attacks.

Summary

The USA-PATRIOT Act was passed as a response to the September 11, 2001 terrorist attacks. The Act significantly expanded the law enforcement’s surveillance and investigative powers. Privacy advocates argue that it represents one of the most significant threats to civil liberties, privacy and democratic traditions in US history.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- USA-PATRIOT Act (III.B.b.)
USA-PATRIOT Act Controversies

The terrorist attacks against the US on September 11, 2001 instigated a sea change in US policy on gathering intelligence to prevent further attacks. About a month after the September 11 attacks, Congress passed a new counterterrorism law known as the USA-PATRIOT Act 2001.

What does the USA-PATRIOT Act do?

This controversial act revised and consolidated counterterrorism laws post-9/11 to strengthen domestic law enforcement investigatory authority, including sweeping surveillance and search powers. Some claim the elimination of judicial oversight ensures that these powers are not abused. In general terms, the Act consolidates and reinforces existing laws to improve federal resources to enable those fighting the war on terror to intercept communications and acquire intelligence to prevent what is considered modern-day terrorism.

The Act takes into account new technologies which enable acts of cyber-terrorism; prohibits the Act of knowingly harboring a terrorist; and provide law enforcement with the ability to delay the notification of a court-approved search warrant in order to prevent a suspect from destroying evidence or fleeing.

Most controversial provisions

The Act’s most controversial provisions include:

- Information sharing – Information from criminal probes may be shared with intelligence agencies and other parts of the government.
- Roving wiretaps – A single wiretap authorization may cover multiple devices, eliminating the need for separate court authorizations for a suspect’s mobile phone, PC and Blackberry, for instance.
- Access to records – Facilitates access to business records in foreign intelligence investigations.
- Foreign intelligence wiretaps and searches – Decreases prerequisites for launching foreign intelligence wiretaps and searches.
- Sneak-and-peek warrants – Allows so-called sneak-and-peek warrants, which allow authorities to search a home or business without immediately notifying the target of a probe.
- Material support – Expands the existing ban on giving “material support” to terrorists to include “expert advice or assistance.”
The Act affected a number of constitutional provisions. Arguably, the laws most tangible impact has been on the Fourth Amendment, which protects individuals from unreasonable searches and seizures. The Act increases the government’s surveillance authority in four key areas:

1. Records searches – Expanded government ability to look at records on an individual’s activity being held by third parties.
2. Secret searches – Expands government’s ability to search private property without notice to the owner.
3. Intelligence searches – Expands a narrow exception to the Fourth Amendment that had been created for the collection of foreign intelligence information.
4. Trap-and-trace searches – Expands another Fourth Amendment exception for spying that collects “addressing” information about the origin and destination of communications, as opposed to the content.

According to the American Civil Liberties Union,

“… there is little evidence that the Patriot Act has been effective in making America more secure from terrorists. However, there are many unfortunate examples that the government abused these authorities in ways that both violate the rights of innocent people and squander precious resources… The American Civil Liberties Union encourages Congress to exercise its oversight powers fully, to restore effective checks on executive branch surveillance powers and to prohibit unreasonable searches and seizures of private information without probable cause based on particularized suspicion.”

The nation remains divided over the Patriot Act, as revealed in a Pew Research Center poll conducted in February 2011. The poll found that 34 percent believe that the law goes too far and actually poses a threat to civil liberties, while 42 percent consider it a necessary tool that helps the government find terrorists. This was compared to 2004 results in which 39 percent of respondents thought the Act went too far, and 33 percent believed it necessary.

Extension of USA-PATRIOT Act

In May 2011, just minutes before the deadline, President Obama signed a four-year extension of the USA-PATRIOT Act. While most of the Act is permanent law, there are certain sections which must be renewed periodically because of concerns that they could be used to violate privacy rights. The measure extends the legal life of the following provisions:

- Roving wiretaps, authorized for a person rather than a communications line or device
- Court-ordered searches of business records
- Surveillance of non-American “lone wolf” suspects without confirmed ties to terrorist groups
Summary

The USA-PATRIOT Act (also referred to as the Patriot Act) was passed in a post-9/11 climate and aimed to strengthen federal anti-terrorism investigation. This article takes a look at some of the controversial provisions within the Act.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Other changes after USA-PATRIOT (III.B.b.i.)
Privacy Protection Act of 1980

The Privacy Protection Act of 1980 (PPA) protects journalists from being required to turn over to law enforcement any work product and documentary materials — including sources — before dissemination to the public. Often, it’s journalists working on stories that are highly controversial or about criminal activity that need the protection of the PPA the most. The Act preserves journalistic freedom to publish information under the First Amendment, without government intrusion.

Why do we need the PPA of 1980?

The Act represents Congress’ response to Zurcher v. Stanford Daily (1978). In this case, the police conducted a warranted search of the Stanford Daily’s newsroom, looking for photos of a demonstration at which police officers were injured. Daily staff attended and photographed the violent demonstration and ran a story with the photos. The police intended to obtain unpublished photos which investigators could then use to identify and prosecute demonstrators. Their search did not uncover new photos of the event, other than those already published.

A federal district court found the search was unlawful and dismissed the police’s argument that the First Amendment has no effect on the Fourth Amendment. The Court of Appeals affirmed per curiam the District Court’s finding that the search was illegal. However, the Supreme Court of the US held that neither the First nor Fourth Amendment prohibited this search.

Two years after the Court ruled in Zurcher, Congress passed the federal Privacy Protection Act (1980) to overrule Zurcher and recognize the need of journalists to gather and disseminate the news without fear of government interference. With a few exceptions, the PPA forbids all levels of law enforcement from searching for and seizing journalists’ work product and documentary materials.

What does the PPA do?

Essentially, the PPA prohibits government officials from searching or seizing the writings and documents of people “reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication.” Such materials can be seized if there is probable cause to believe the publisher is involved in the criminal offence.
Basically, the PPA prevents investigators from searching newsrooms to uncover information or sources that a news organization has assembled. It forces law enforcement to use subpoenas or voluntary cooperation to obtain evidence from those engaged in activities protected by the First Amendment.

The PPA defines “work product” materials as materials that are “prepared, produced, authored, or created” for the purpose of communicating such materials to the public. This definition is also extended to a reporter’s “mental impressions, conclusions, opinions or theories” that concern such material. As long as a reporter intends to disseminate information in his/her possession to the general public, any form of a reporter’s “work product” should be protected from search and seizure.

The PPA defines “documentary materials” quite broadly as “materials upon which information is recorded.” This includes things like photographs, motion pictures, audiotapes, and film negatives. Computer disks are also considered documentary materials, along with other “mechanically, magnetically or electronically recorded tape, card or disk.”

Exceptions to the PPA

Searches are permitted when the person who has the information is suspected of committing the criminal offence or “There is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to, a human being.”

Searches of documentary materials are permitted when the mere notice of a “subpoena [for documents] would result in the destruction, alteration, or concealment of such materials,” or when, after no response to a subpoena, the government representative has exhausted “all appellant remedies” or justice would be threatened by further delay.

Searches by government officials on both state and federal levels are covered under the PPA. A number of states have also reiterated or strengthened protection against these searches under state law. These states are: California, Connecticut, Illinois, Nebraska, New Jersey, Oregon, Texas, Washington and Wisconsin.

Summary

This article takes a look at the Privacy Protection Act of 1980 (PPA), which covers searches and seizures by government officers and employees in connection with investigation or prosecution of criminal offenses. Basically, the PPA prevents investigators from searching newsrooms to uncover information or sources that a news organization has assembled.
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Privacy Protection Act of 1980 (III.C.a.i.)
e-Discovery Basics

Electronic discovery (e-discovery) refers to the identification, preservation, collection, processing and analysis, review and production of electronically stored information in preparation for litigation, regulatory investigation or audit. The volume of electronic information involved in a single case may vary from hundreds to millions of records, the vast majority of these created electronically. It’s important to understand and adopt the best practices and methodologies for managing electronic records.

Electronically Stored Information (ESI)

These days, over 90 percent of new information is being stored electronically. Given this reality, key evidence is more likely to be stored electronically than as a hard copy. Furthermore, an email or other electronic document will contain more information than provided in a printed paper copy. Not unlike fingerprints on a handwritten note, an email contains metadata that provide a wealth of information. Lawyers are increasingly required to access electronically stored information (ESI) during the discovery process.

Metadata contained in ESI may reveal things like the data the document was created, the identities of its author and editors, the distribution route and the history of editorial changes. Authenticated computer files are considered “best-evidence,” as they are either original documents or exactly the same as the original document. ESI can be found in various and multiple locations and formats, making it difficult for all copies of a given document to be intentionally destroyed. Without a doubt, the most voluminous type of evidence is email, which exist only in an electronic format and are normally “unsanitized.”

It’s important to note that ESI can be more difficult to locate and capture than traditional paper documents, which are more routinely found in only one or two locations. Also, ESI can be easily and unknowingly destroyed in the normal course of business by turning on a computer, saving new files, or the rotational reuse of backup tapes.

E-Discovery Law in the US

E-discovery law is developing at a rapid rate in the US, being driven by both regulations and case law. There have been numerous multi-million dollar lawsuits and many other smaller cases that have shone a spotlight on e-discovery issues.

US e-discovery rules focus on the notion that any non-privileged information relevant to a claim or a defense must be produced on a request for discovery. The sanctions associated with the failure to produce requested information are so significant that all parties to a litigation matter are strongly advised to take immediate steps to preserve potentially relevant data.
Most corporations are encouraged to develop stringent document retention policies in order to provide reasonable limitations on the quantity of electronic information available for potential production. New rulings regularly impose heavy fines and other sanctions on corporations that have not properly preserved potentially relevant documents, or where a failure to destroy outdated information has resulted in extremely high and otherwise avoidable e-discovery costs.

Current e-Discovery Issues

The collection and review of electronic information raises unique issues with regard to privacy and privilege, as computers may be used to store personal files as well as privileged and non-privileged business-related files in essentially the same location. In the corporate context, courts have not hesitated to find that employees have little, if any, privacy rights with regard to the files on company computers.

Spoliation and the duty to preserve represent one of the hottest issues in US courtrooms. Courts routinely sanction both plaintiffs and defendants for the failure to preserve and produce electronic evidence. While it is difficult to classify cases by their e-discovery issues, it is estimated that well over half of identified electronic discovery case opinions pertain to ESI production, preservation and spoliation.

The failure to respond appropriately to e-discovery requests may be extremely costly in terms of fines and adverse jury inferences. However, responding to requests may also be expensive. An estimate puts the cost of restoring and reviewing emails at $2/email. For giants like Microsoft, which receives an average of 25-30 million emails every day, the cost of a broadly based e-discovery request could be staggering.

Summary

This article takes a look at electronic discovery (e-discovery), which is the identification, preservation, collection, processing and analysis, review and production of electronically stored information in preparation for litigation, regulatory investigation or audit.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Civil litigation and privacy – electronic discovery (III.C.b.)
CIPP Applied – e-Discovery

Electronic Discovery, or e-Discovery, is the digital analog to a court request for documents and files pertaining to a proceeding. As with anything digital, the courts expect discovery times in days and weeks, versus the months (years) given for paper files. Punishments for failure to produce could be regulatory, legislative, or may even include court based consequences such as contempt charges.

In a recent survey by Information Security Magazine, only 28 percent of respondents knew how they would handle an eDiscovery request. Even knowing where to look seems a daunting task. I have trouble at times finding a matching pair of socks in a 2’ x 3’ drawer.

Well-prepared companies develop policies. Some buy eDiscovery or search software. Even better prepared Configuration Managed CMMI level companies define procedures. They begin data inventories. This is where I see it becomes interesting…

A typical company has a lot more data lying around than they really expect. Think about a day in the life of an enterprise. Email, IM, network file shares, database records, log files, security devices, executive summary reports, backup tapes, and the list goes on. That’s not even considering end workstations, laptops or PDAs (where the majority of people I know do their work) or decommissioned hardware (there’s still data on those things), CD-R/DVD-Rs or other removable media. I’m sure you see the point; there are a ton of sources. That’s only half the problem.

If you ever learn about government data classification, there are three reasons something’s classified. It contains important information, the source of the information is important, or the information amalgamated from various parts into one location makes it important. This is why identity thieves hack corporate databases; it’s the proverbial is “or until now the most consolidated repository.

So now let’s offer them a juicier target! Put the map to Curly’s Gold, and the Lost Dutchman’s mine, and all the rest of them in one location. Insiders and outsiders alike should be clambering for it, with the idea that you can pick and choose what’s most interesting. Want the network architecture diagrams? IT admin’s machine, here’s the IP address. Customer Personally Identifiable Information (PII) database? Oracle server’s on the fourth floor want the table configs. Corporate strategy or yet to be released financials, aisle 12…

This is why most government documents become classified. Someone did the hard research and heavy lifting. Anyone that can put their hands on it just has to cite the paragraphs they want to look omniscient, or at least very well informed. A perfect example is an enterprise firewall rule set; the outgoing Port Allows from one site doesn’t provide much; couple the complete configs of all of the boundary protections and you have something someone may do harm with.

To counteract the centralized data repository threats from an InfoSec standpoint, we will put in place perimeter protections, audit the systems for hackers and insiders alike, instantiate policies as far as who should access what information with what sorts of separation of duties, etc… Ten
years ago, this was all pretty cutting edge and Wild West gunslinger-esque. Today, it’s called industry best practices.

My question becomes one of Information Privacy and Policy: who’s keeping the snoops from browsing the celebrity hospital records? Or placing obviously needed controls prior to simply supplying all information available? Or when it’s just flat out wrong?

Seriously, who should have access? One of the better known companies that had to tackle this problem: Google. Every search made with Google winds up in a very big database with information such as IP addresses, search terms, etc. (ever read the privacy policy?). This much data in one spot is tempting, but it’s somewhat anonymized (recently), and according to Google security folks I’ve talked to, very well controlled by corporate policy and enforced with security protections. Only a handful of people have access, physical and logical. I would say Google may be the exception.

Obviously, the end court will receive a redaction: if it’s pertinent to the case, they’re entitled to it by law. But someone has to do the sorting. Is it the attorneys, the IT staff, the management? Current insider threats are hampered somewhat by the hard work of inventory and cataloging; they target the low-hanging fruit. Now, the most accessible jobs, probably interns and juniors, may be sorting the records considered for evidence.

What happens when the collected information comes from a company you worked for the past twenty years, and it comprises your whole life story, laid out on a silver hard drive platter? If they get parts of it wrong, producing inaccurate reports that slander your good name by opening lines of question well outside the original case? The Fair Credit Reporting Act legislation protects your credit info with the credit bureaus.

Nothing right now controls eDiscovery accuracy. That’s not that big of a deal, with the idea being this info will ONLY be used in judicial proceedings or congressional hearings (steroids in baseball), and in those you start down the witness credibility path (I guess data creator credibility would be more accurate).

Do we need more legislation for protecting these huge information stores and location roadmaps, or can we rely even more heavily on information security professionals to instantiate further best practices? I’m a smaller government kind of guy, so I’d prefer industry policing.

Unfortunately with the exception of the Payment Card Industry’s (PCI) work, the government has stepped in to clean up most of the debaucherous messes self-regulatory models let through. Typically, once laws are enacted, industry conforms to the letter, doing the bare minimum to comply rather than what would be in the best interest of their customers. Just think of how far HIPPA falls short.

Obviously, there’s a great deal of work to be done with eDiscovery. Maybe the attorneys will make sure it’s done in the right way?

Hey, I found that black and grey argyle I was looking for…
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Civil litigation and privacy – electronic discovery (III.C.b.)
End-of-Chapter Review

Right to Financial Privacy Act (RFPA)

- Allows the federal government to request individual financial records without restriction.
- Offers weaker protections for customer financial privacy than those granted under the Fourth Amendment.

Bank Secrecy Act of 1970 (BSA)

- Helps US government monitor and prevent possible money laundering schemes
- Financial institutions to keep records about customer transactions, submit reports to federal government
- CTR = currency transaction report
- CMIR = currency and monetary instrument report
- SAR = suspicious activity report

Electronic Communications Privacy Act of 1986 (ECPA)

- Expands government restrictions on wiretaps to include electronic communications.
- Expands the types of crimes that allow law enforcement to intercept communications.
- Title III – federal crime to engage in wiretapping or electronic eavesdropping; to possess such equipment; to disclose information obtained through such activities.
- Stored Communications Act (SCA) – bans surreptitious access to communications at rest.

Communications Assistance for Law Enforcement Act (CALEA)

- Passed in 1994 to facilitate law enforcement wiretapping of telephone networks.
- August 2004: FCC released a Notice of Proposed Rule Making (NPRM) to expand CALEA.
- August 2005: FCC announces a Final Rule, which includes broadband Internet access providers and managed VoIP systems.
Foreign Intelligence Surveillance Act 1978 (FISA)

- Requires government to obtain search warrants and wiretap orders from a court, even when investigating foreign threats to national security.

USA-PATRIOT Act

- Response to 9/11 attacks
- Subpoena of ISPs to access information
- “Sneak and peek” warrants = delayed notice of search warrants
- Expanded wiretapping activities: roving wiretaps, surveillance of packet switched networks
- Expanded duration of search and surveillance orders
- Increased “terrorism-related” investigations
- Arguably violates rights under the Fourth Amendment

Privacy Protection Act of 1980 (PPA)

- Protects journalists from having to give law enforcement authorities any work product or documentary materials (including sources) before dissemination to the public.
- Preserves First Amendment rights.

E-Discovery

- Identification, preservation, collection, processing and analysis, review and production of electronically stored information (ESI) in preparation for litigation, regulatory investigation or audit.
- Digital analog to a court request for documents and files pertaining to a proceeding.
- ESI = 90 percent of new information (e.g. emails or digital documents)
Chapter Five

CIPP Prep Guide
CIPP/US Concentration: Workplace Privacy

Introduction to Workplace Privacy

Human Resources & Workplace Privacy

The workplace can be an environment where many types of privacy-invasive monitoring may take place. This may include drug testing, closed-circuit video monitoring, internet monitoring and filtering, email monitoring, instant message monitoring, phone monitoring, location monitoring, personality and psychological testing, and keystroke logging. There is a wide variety of reasons why employers choose to monitor, including addressing security risks, sexual harassment and to ensure acceptable performance of employees. Developments in technology have also increased employers’ ability to monitor employees both at work and outside of work.

Challenges in Workplace Privacy

Changes in the workplace have made it necessary to reassess boundaries in the employer-employee relationship. In the US, many workers are not protected with due process guarantees against arbitrary discharge. Without state law or contract, employers can often dismiss an employee for any reason, or no reason, even if the decision to terminate is based on false information.

Increased employee monitoring activities raise the risk that false inferences can be drawn about employee conduct. An employee network-monitoring appliance can detect access to inappropriate sites, but not the intention of the employee. New monitoring tools definitely have the potential to draw false inferences. For this reason, it’s even more important for employees to have basic due process protections; the right of notice of the violation and an opportunity to be heard.

US law includes very few privacy protections for workers. There are certain situations where an employee may have a due process right to access, inspect, or challenge information collected or held by the employer. A few state and federal laws grant employees limited rights. For example, under federal law, private-sector employees cannot be subjected to a polygraph examination. However, there are no general protections of workplace privacy except where an
employer acts tortuously, where the employer violates the employee’s reasonable expectation of privacy.

Major Workplace Privacy Issues

There are several main issues under workplace privacy in which privacy rights have been established, whether in federal, state or local law. These issues include:

- **Personnel Records** – Employees generally have a right to privacy in their personnel records. Employers are normally not permitted to disclose personnel records to third parties without a legal obligation to do so, or the employee’s permission. This is protected by state statutes, codes or judicial case law. In most states, employees have the right to request access to their personnel files upon proper notice.

- **Social Security Numbers** – In order to respond to an increase in identity theft, a number of statutory laws have been enacted to protect the privacy of social security numbers. State laws limit and/or prohibit the use of all or part of SSNs as computer passwords or ID numbers. Certain laws also limit whether and to what extent SSNs can be used on itemized wage statements.

- **Monitoring and Eavesdropping** – Extensive anti-eavesdropping laws prohibit tapping into telephone conversations, voicemail systems and electronic communications systems. Camera surveillance is also subject to various legal requirements regarding notice and disclosure to employees.

- **Medical Records** – Federal and state laws protect the privacy of employee medical information and require various disclosures about how the information is maintained, who has access to it and how it may be used.

- **Drug Testing** – Employers who conduct drug testing are required to maintain the confidentiality of the test.

- **Background Screening** – Employers who conduct background checks as part of the employment process must maintain the confidentiality of the background information received. There are notice requirements if this information is used to make an adverse employment decision.

PPSC Report 1977

The Privacy Protection Study Commission (PPSC) released a report covering workplace privacy in 1977. The report recognized that employers collect a broad range of information on their workers. It forced on delineating lines of fairness on the collection and use of employee information. The report recognized that much had changed since the development of common law employment norms.
American employees do not always have the power to bargain the terms of their employment and the PPSC approach recognized that “People with a given employment status must adhere to many terms of employment set by the organization they work in if they are to work at all.”

The PPSC pursued three public policy objectives:

1. Minimize intrusiveness in hiring, specifically to reduce the practice of obtaining information about the employee from a third party (e.g. credit reporting agency).
2. Maximize fairness, by reducing the arrest information and ensuring that information collected is accurate, complete and timely.
3. Create a legitimate and enforceable expectation of confidentiality in employment records.

In the report, the PPSC made 34 recommendations to meet these objectives.

Summary

Employee monitoring includes a broad range of activities, including drug testing, closed-circuit video monitoring, internet monitoring and filtering, email monitoring, instant message monitoring, phone monitoring, location monitoring, personality and psychological testing, and keystroke logging. This article takes a look at employee monitoring and the US approach to workplace privacy.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Workplace privacy concepts – HR management (IV.A.a.i.)
Workplace Privacy: Trends & Developments

It’s been estimated that in the United States a staggering 20 million workers are electronically monitored on the job. Employee surveillance includes anything from keystroke counting; telephone service observation (including call duration; time between, and number of calls); telephone call accounting; “peeking” on workers’ computer screens and email; and the use of “active” badges that track an employee’s movements and location.

According to Michael Levy:

“As a private employee there are minimal constitutional rights to privacy. The principle of State action in the fourteenth amendment gives limited constitutional privacy rights to those in the private sector. Even for public employees and those states that have explicit privacy provisions in their constitutions the difficulty in claiming an invasion of privacy revolves around the test of a “reasonable expectation of privacy” in the workplace.”

This article takes a look at how some trends and statistics in employee monitoring and workplace privacy.

Trends in Employee Monitoring

Numerous studies and reports indicate that monitoring employee behavior – both in and out of the workplace – has undergone a dramatic increase in recent years. This includes an increase of scope and type of surveillance. Indeed, personal behavior is no longer out-of-bounds, as companies have been known to enforce rules limiting coworkers’ dating, as well as smoking and drug use regulations.

Employers have been combining technology with policy to manage productivity and minimize litigation, security and other risks. In order to strengthen compliance with rules and policies, over a quarter of employers have fired workers for misusing email and nearly a third of employers have fired employees for misusing the internet, according to the American Management Association’s Electronic Monitoring & Surveillance survey results. This study found that over half of employers polled monitored all employees’ internet usage, while a quarter of them admitted to storing and reviewing all employees’ computer files. It’s important to note that the AMA’s study included both private and public sector employees.

Blind Spots

These trends have been the focus of employees and civil liberties advocates. If one were to disregard the ethical issues of employee surveillance, errors in monitoring practices would still have significant repercussions on workers. For instance, information gathered from surveillance practices may be used to incorrectly inform decisions that may impact a worker’s career options and advancement.
However, employees’ invasion of privacy claims has garnered little more success than those brought under the ECPA or state wiretapping laws. Most courts have declined to find an employer’s monitoring of employee emails or computer usage an infringement of an individual’s right to privacy in the workplace. Courts typically find that employees have no reasonable expectation of privacy for communications voluntarily transmitted or saved on an employer’s network. Case law shows that even if there were a reasonable expectation of privacy, the intrusion upon seclusion is not highly offensive.

Legislative Attempts

The Privacy for Consumers and Workers Act was been introduced in Congress in 1993, but never passed. The Act provided that electronic monitoring of employees could only occur if the employer complied with specific notice requirements. The only exception to this was “If an employer had a reasonable suspicion that any employee [was] engaged in conduct which violated criminal or civil law or constituted willful gross misconduct,” and if such misconduct adversely affected “the employer’s interests or the interests of other employees.”

In 2000, the Notice of Electronic Monitoring Act was proposed. It required companies to notify workers if their email messages, Internet usage, or phone usage was being monitored by the company. Notice required by the Act would include the type of monitoring taking place, the means, the type of information that would be gathered, including non-work related information, the frequency of the monitoring and how the information would be used. Like the Privacy for Consumers and Workers Act, this bill also was not passed.

Despite this, there are many privacy advocates who argue that a uniform federal law is still a good idea. The working model should be one based on minimum intrusiveness. Companies would then be required to justify each encroachment on privacy with a valid business purpose. Remedies would be made available to employees, should they find themselves working for a company that violates their basic privacy rights.

Summary

This article takes a look at how some trends and statistics in employee monitoring and workplace privacy. It also discusses two legislative attempts at employee protection – the Privacy for Consumers and Workers bill (1993) and the Notice of Electronic Monitoring bill (2000).
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Workplace privacy concepts – HR management (IV.A.a.i.)
Workplace Privacy: Regulation at the US Department of Labor

By law, US federal agencies are required to ensure the protection of the personally identifiable information (PII) they collect, store and transmit. In light of the current digital environment, government agencies are collecting more and more personal information. Highly publicized events of abuse, misuse and inadvertent errors in agency management of PII has fueled public concern about the government's ability to protect private or sensitive information. This has resulted in increasing scrutiny and compliance expectations regarding federal privacy laws and regulations, which affects federal employees at all levels.

This article takes a look at how the US Department of Labor regulates privacy issues.

Department of Labor

The US Department of Labor (DoL) must appropriately protect the information contained within its information systems, including PII. In order to meet this objective, the DoL has developed a Privacy Impact Methodology to assess whether a system containing PII meets legal privacy requirements.

The DoL’s Methodology looks something like this:

Characterization of the Information

- What are the sources of the PII in the information system?
- What is the PII being collected, used, disseminated, or maintained?
- How is the PII collected?
- How will the information be checked for accuracy?
- What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Uses of the PII

- Describe all uses of the PII
- What types of tools are used to analyze the data and what type of data may be produced?
- Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?
- If the system uses commercial or publicly available data, please explain why and how it is used.

Retention

- How long is information retained in the system?
- Has the retention schedule been approved by the DoL agency records officer and the National Archives and Records Administration (NARA)?
• How is it determined that PII is no longer required?
• What efforts are being made to eliminate or reduce PII that is collected, stored or maintained by the system if it is no longer required?

Internal Sharing and Disclosure

• With which internal organization(s) is the PII shared, what information I shared, and for what purpose?
• How is the PII transmitted or disclosed?

External Sharing and Disclosure

• With which external organization(s) is the PII shared, what information is shared, and for what purpose?
• Is the sharing of PII outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, describe under what legal mechanism the program or system is allowed to share the PII outside of the DoL.
• How is the information shared outside the Department and what security measures safeguard its transmission?

Notice

• Was notice provided to the individual prior to collection of PII?
• Do individuals have the opportunity and/or right to decline to provide information?
• Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Access, Redress, and Correction

• What are the procedures that allow individuals to gain access to their information?
• What are the procedures for correcting inaccurate or erroneous information?
• How are individuals notified of the procedures for correcting their information?
• If no formal redress is provided, what alternatives are available to the individual?

Technical Access and Security

• What procedures are in place to determine which users may access the system and are they documented?
• Will Department contractors have access to the system?
• Describe what privacy training is provided to users, either generally or specifically relevant to the program or system?
• What auditing measures and technical safeguards are in place to prevent misuse of data?
Technology

- What stage of development is the system in and what project development life cycle was used?
- Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

An example of the DoL’s Privacy Impact Methodology in use may be found here.

Summary

US federal agencies are legally required to protect the personally identifiable information (PII) they collect, store and transmit. This article takes a look at how the US Department of Labor (DoL) regulates privacy issues.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- US agencies regulating workplace privacy issues – Department of Labor (IV.A.b.ii.)
Workplace Privacy: Equal Employment Opportunity Commission

By law, US federal agencies are required to ensure the protection of the personally identifiable information (PII) they collect, store and transmit. In light of the current digital environment, government agencies are collecting more and more personal information. Highly publicized events of abuse, misuse and inadvertent errors in agency management of PII has fueled public concern about the government’s ability to protect private or sensitive information. This has resulted in increasing scrutiny and compliance expectations regarding federal privacy laws and regulations, which affects federal employees at all levels.

This article takes a look at how the Equal Employment Opportunity Commission (EEOC) handles privacy issues.

EEOC Assessment System: Privacy Impact Assessment

The following laws and regulations establish specific requirements for the confidentiality, integrity and availability of the data processed, stored and transmitted by the EEOC Assessment System (EAS):

- Computer Fraud and Abuse Act of 1984
- Federal Information Security Management Act of 2002
- OMB February 1996 Circular A-130, Appendix III
- Paperwork Reduction Act of 1980
- Privacy Act of 1974
- Title VII of the Civil Rights Act of 1964
- Equal Pay Act of 1963
- Age Discrimination in Employment Act of 1967
- Title I and V of the Americans with Disabilities Act of 1990
- EEOC Order 240.005, EEOC Information Security Program
- Information Security Responsibilities of EEOC Employees
- EEOC Order 150.003, Privacy Act of 1974, as amended

This is what an EEOC privacy assessment would look like:

Data in the System

- Generally describe the information to be used in the system in each of the following categories: complainant; company; EEOC employee; other.
- What are the sources of the information in the system?
- How will data collected from sources other than EEOC records and the complainant or company be verified for accuracy?
- Are the data elements described in detail and documented? If yes, what is the name of the document?
• How will the data be used by the agency? Who is responsible for assuring proper use of the data?

Access to the Data

• Who will have access to the data in the system (e.g. users, managers, system administrators, developers, other)?
• How is access to the data by a user determined? Are criteria, procedures, controls and responsibilities regarding access documented?
• Will users have access to all data on the system or will the users’ access be restricted?
• What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?
• Do other systems share data or have access to data in this system? If so, explain. Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?
• Will other agencies share data or have access to data in this system (e.g. international, federal, state, local, other)?
• How will the system ensure that agencies only get the information they are entitled to under applicable statutes or regulations?

Attributes of the Data

• Is the use of the data both relevant and necessary to the purpose for which the system is being designed?
• Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?
• If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
• How will the data be retrieved? Can it be retrieved by a personal identifier? If yes, explain. What are the potential effects on the due process rights of individuals: consolidation and linkage of files and systems; derivation of data; accelerated information processing and decision-making; use of new technologies. How are the effects to be mitigated?

Maintenance of Administrative Controls

• Explain how the system and its use will ensure equitable treatment of individuals. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?
• What are the retention periods of data in this system?
• Is the system using technologies in ways that the EEOC has not previously employed?
• Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.
• Under which Systems of Record notice (SOR) does the system operate?
An example of an EEOC Assessment System Privacy Impact Assessment may be found here.

Summary

By law, US federal agencies are required to ensure the protection of the personally identifiable information (PII) they collect, store and transmit. This article takes a look at how the US Equal Employment Opportunity Commission (EEOC) handles data to ensure that privacy laws and regulations are being respected.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

Workplace Privacy: National Labor Relations Board

By law, US federal agencies are required to ensure the protection of the personally identifiable information (PII) they collect, store and transmit. In light of the current digital environment, government agencies are collecting more and more personal information. Highly publicized events of abuse, misuse and inadvertent errors in agency management of PII has fueled public concern about the government’s ability to protect private or sensitive information. This has resulted in increasing scrutiny and compliance expectations regarding federal privacy laws and regulations, which affects federal employees at all levels.

This article takes a look at how the National Labor Relations Board (NLRB) handles privacy issues.

NLRB’s Privacy Impact Assessments

Section 208 of the e-Government Act of 2002 requires federal agencies to conduct a Privacy Impact Assessment (PIA) before developing or procuring information technology systems or projects that collect, maintain or disseminate PII about members of the public.

The NLRB has conducted PIAs on the following systems:

- Back Pay System
- Case Activity Tracking System
- Judicial Case Management System
- Litigation Information on the Network
- Next Generation Case Management System
- Office of the Inspector General Investigative Files
- Paper Check Conversion Over the Counter
- Treasury Offset Program
- Work in Progress

This is what an NLRB Privacy Impact Assessment would include:

Nature of the System

- What is the system called?
- Provide a generalized, broad description of the system and its purpose (i.e. what does this system do? What function does it fulfill?)
- Describe the stage of development of this system.
- Is this system required by law or Executive Order?
Data in the System

- Will this system contain personal data elements?
- List the personal data elements or types of data elements that the system will contain.
- What are the sources of the personal information in the system?
- Are the personal data elements described in detail and itemized in a record layout or other document?
- Review the list of personal data elements you currently collect. Is each data element essential to perform some official function?

Verifying Data

- For data collected from sources other than NLRB records and the record subject him/herself, describe how the data will be verified for accuracy, completeness, relevance and timeliness.
- Describe your procedures for determining if data have been tampered with by unauthorized persons.

Access to the Data

- Who will have access to the data in the system (e.g. users, managers, system administrators, developers, others)?
- How is right of access to the data by a user determined?
- Are criteria, procedures, controls and responsibilities regarding access documented?
- What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?
- Do other systems share data or have access to data in this system?
- Will other non-NLRB agencies share data or have direct access to data in this system (e.g. international, federal, state, local, other)?
- How will the system ensure that agencies only get the information they need to fulfill their official functions?
- Who will be responsible for protecting the privacy rights of individuals and employees affected by the interface between agencies?
- Who is responsible for assuring proper use of the data?

Attributes of the Personal Data

- Is the use of the personal data both relevant and necessary to the purpose for which the system is being designed?
- Will the system derive new data or create previously unavailable data about an individual through a data aggregation process?

Maintenance of Administrative Controls

- Explain how the system and its use will ensure equitable treatment of individuals.
• Explain any possibility of disparate treatment of individuals or groups.
• What are the retention periods for the data in this system?

Interface with Privacy Act Systems of Records

• Does this system currently operate under an existing NLRB or Government-Wide Privacy Act system of records?
• Provide the identifying number and name of each system.
• If an existing NLRB Privacy Act system of records is being modified, will the system notice require amendment or alteration?
• If the system currently operates under an existing Government-Wide Privacy Act system of records notice, are your proposed modifications in agreement with the existing notice?
• If not, have you consulted with the government agency that “owns” the government-wide system to determine if they approve of your modifications and intend to amend or alter the existing notice to accommodate your needs?

An example of an NLRB Privacy Impact Assessment can be found here.

Applying the National Labor Relations Act

During 2011 and 2012, the NLRB’s Acting General Counsel published three Advice Memos, which reflected his views on the application of the National Labor Relations Act (NLRA) to social media policy provisions and employers’ discipline based on employees’ personal social media content. Some of the major opinions and views to come out of these memos are outlined below:

• Employers cannot prohibit damaging statements about the company or its employees.
• Employees are prohibited from discussing a coworker’s health condition. Employers ought to promote policy that prohibits employees whose job duties entail access to employees’ health information from disclosing that information in any manner, including via social media outlets.
• Employers could promote policy that prohibits employees from disclosing compilations of payroll data when properly characterized as confidential business information.
• Employees have a protected right to use and disclose coworkers’ contact information (e.g. names, addresses, phone numbers, email addresses), for “organizational purposes,” as long as the information is not obtained from the employer’s files.
• Employers are permitted to establish rules intended to promote a “civil and decent workplace.” As long as a reasonable employee would understand the rule – for instance a rule requiring appropriate business decorum in communications – to achieve the above purpose, such rules are acceptable to the NLRB.
Summary

US federal agencies are legally required to ensure the protection of personally identifiable information (PII) they collect, store and transmit. This article takes a look at how the National Labor Relations Board (NLRB) deals with privacy issues.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- US agencies regulating workplace privacy issues – National Labor Relations Board (IV.A.b.iv.)
Occupational Safety and Health Act

In 1971, Congress passed the Occupational Safety and Health Act to ensure worker and workplace safety. Their goal was to ensure that employers provide their employees with a workplace free from recognized hazards to safety and health, for instance, exposure to toxic chemicals, excessive noise levels, mechanical dangers, heat or cold stress, or unsanitary conditions.

To establish standards for workplace health and safety, the OSHA created the National Institute for Occupational Safety and Health (NIOSH) as the research institution for the Occupational Safety and Health Administration (OSHA). OSHA represents a division of the US Department of Labor that oversees the administration of the Act and enforces standards in all fifty states.

A closer look at the Act

The Occupational Safety and Health Act was enacted to “assure safe and healthful working conditions for working men and women.”

While the Occupational Safety and Health Act is administered through the Department of Labor, many states have their own occupational health and safety laws. Generally, the federal Act requires employers to:

- Allow OSHA inspections without notice or as a result of an employee complaint.
- Provide workers with information on OSHA protection, via workplace posters and other notifications.
- Provide workers with information on identifying hazardous substances in the workplace and training on how to treat injuries from these substances.
- Provide workers with information on first aid procedures, and protection against blood-borne pathogens in the workplace.
- Provide workers with training on how to deal with fires and other emergencies.

The Act also requires that employers do not take action against employees who file complaints alleging violations of the Act.

“Privacy Concern” Cases

The OSHA explains to employers that there are certain record-keeping situations which would be considered “privacy concern” cases. In such situations, employers are prohibited from including the employee’s name on the records or forms for privacy reasons. Instead, they are instructed to enter “privacy case” in the space normally reserved for the individual’s name. This is done to protect the privacy of the injured or ill employee when another employee, a former employee, or an authorized employee representative is provided access to the log.
Employers are also required to keep a separate, confidential list of the case numbers and employee names for privacy concern cases so they can update the cases and provide the information to the government, if required.

In order to determine if an injury or illness would be considered a “privacy concern” case, employers are asked to consider the following:

- An injury/illness to an intimate body part or the reproductive system
- An injury/illness resulting from sexual assault
- Mental illness
- HIV infection, hepatitis, or tuberculosis
- Needlestick injuries and cuts from sharp objects that are contaminated with another person’s blood or other potentially infectious material
- Other illnesses, if the employee voluntarily requests that his/her name not be entered on the log

Summary

US federal agencies are legally required to ensure the protection of personally identifiable information (PII) they collect, store and transmit. This article takes a look at the Occupational Safety and Health Act and how the Occupational Safety and Health Administration (OSHA) deals with privacy issues.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- US agencies regulating workplace privacy issues – Occupational Safety and Health Act (IV.A.b.v.)
Workplace Privacy: US Securities and Exchange Commission

By law, US federal agencies are required to ensure the protection of the personally identifiable information (PII) they collect, store and transmit. In light of the current digital environment, government agencies are collecting more and more personal information. Highly publicized events of abuse, misuse and inadvertent errors in agency management of PII has fueled public concern about the government’s ability to protect private or sensitive information. This has resulted in increasing scrutiny and compliance expectations regarding federal privacy laws and regulations, which affects federal employees at all levels.

This article takes a look at how the US Securities and Exchange Commission (SEC) handles privacy issues.

PIAs at the SEC

The e-Government Act of 2002 (Sec. 208) requires federal agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The following outlines why PIAs are conducted and how personally identifiable information is managed in information systems within the SEC.

A PIA should be completed when any of the following activities take place:

- Developing or procuring any new technologies or systems that handle or collect personal information.
- Developing system revisions.
- Imitating a new electronic collection of information in identifiable form for 10 or more persons, consistent with the Paperwork Reduction Act.
- Issuing a new or updated rulemaking that affects personal information.
- Categorizing System Security Controls as “high-major,” or “moderate-major.”

A PIA is not required in the following instances:

- For government-run websites, IT systems, or collections of information that do not collect or maintain information in identifiable form about members of the general public, government employees, contractors, or consultants.
- For government-run public websites where the user is given the option of contacting the site operator for the limited purpose of asking questions or providing comments.
- For national security systems.
- When all elements of a PIA are addressed in a data matching or comparison agreement governed by the computer matching provisions of the Privacy Act.
- When all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use under Title V of the e-Government Act.
When developing IT systems or collecting non-identifiable information for a discrete purposes that does not involve matching with or retrieval from other databases that generate individual or business identifiable information.

For minor changes to an IT system or collection that do not create new privacy risks.

When completing a PIA for the SEC, the system owner is required to respond to privacy-related questions regarding:

- Data in the system (e.g. what data is collected and why it is collected)
- Attributes of the data (e.g. use, accuracy)
- Sharing practices
- Notice of individuals to consent/decline use (e.g. SORN)
- Access to data (i.e. administrative and technological controls)

Section 504 Privacy Rules

In November 2000, the Securities and Exchange Commission announced their adoption of Regulation S-P, which included privacy rules promulgated under section 504 of the Gramm-Leach-Bliley Act (GLBA). Section 504 requires the SEC and other federal agencies to adopt rules implementing notice requirements and restrictions on a financial institution’s ability to disclose nonpublic personal information about customers.

Under the GLBA, a financial institution must provide its customers with a notice of its privacy policies and practices. The institution is prohibited from disclosing nonpublic personal information about a consumer to nonaffiliated third parties, unless the institution provides certain information to the consumer and the consumer has not elected to opt out of the disclosure. The GLBA also requires the SEC to establish appropriate standards for financial institutions to protect customer information. The final rules implement these requirements of the GLBA, with respect to investment advisers registered with the SEC, brokers, dealers and investment companies, which are all considered financial institutions subject to the SEC’s jurisdiction under the GLBA.

Penalties for Privacy Violations

In April 2011, the SEC announced a settlement involving three former brokerage firm executives who were charged with “failing to protect confidential information about their customers.” This represented the first time the SEC assessed financial penalties against individuals charged solely with violations of Regulation S-P, introduced in the section above.
Essentially, the president of the brokerage firm took information from over 16,000 customers without notifying them or providing an opportunity to opt-out. Information included names, addresses, account numbers and asset values. The SEC also found that the firm’s information security procedures were inadequate, even after numerous security breaches which involved stolen company laptop computers and unlawful access to company emails. As a result of the settlement, the firm’s former president and national sales manager were required to pay $20,000 each, and the former chief compliance officer was fined $15,000.

Summary

US federal agencies are required to protect personally identifiable information (PII). This article takes a look at how the US Securities and Exchange Commission (SEC) handles privacy issues, ranging from filing a privacy impact assessment (PIA), to implementing and enforcing Regulation S-P of the Gramm-Leach-Bliley Act (GLBA).

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- US agencies regulating workplace privacy issues – Securities and Exchange Commission (IV.A.b.vi.)
Civil Rights Act of 1964

A civil right is an enforceable right or privilege, which, if interfered with by another gives rise to an action for injury. Civil rights include freedom of speech, press, and assembly; the right to vote; freedom from involuntary servitude; and the right to equality in public places. One of the most prominent civil rights legislation is the Civil Rights Act of 1964.

Civil Rights Act, in brief...

The following outlines the major features of the Civil Rights Act of 1964:

- **Title I: Voting Rights** – This barred unequal application of voter registration requirements, but did not abolish literacy tests sometimes used to disqualify African Americans and poor white voters.
- **Title II: Public Accommodations** – Outlawed discrimination in public accommodations (e.g. hotels, motels, restaurants, theaters) engaged in interstate commerce. Exempt from this are private clubs without defining “private,” thus allowing a loophole.
- **Title III: Desegregation of Public Facilities** – Permitted Justice Department suits to secure desegregation of certain public facilities.
- **Title IV: Desegregation of Public Education** – Encouraged desegregation of public schools and authorized the US Attorney General to file suits to force desegregation. However, it did not authorize busing as a means to overcome segregation based on residence.
- **Title V: Civil Rights Commission** – Addressed procedures for the Commission, broadened its duties and extended its life through January 1968.
- **Title VI: Nondiscrimination in Federally-Assisted Programs** – Authorized (but did not require) withdrawal of federal funds from programs which practiced discrimination.
- **Title VII: Equal Employment Opportunity** – Outlawed discrimination in employment in any business exceeding twenty-five people and creates an Equal Employment Opportunities Commission (EEOC) to review complaints, although it lacked meaningful enforcement powers.
- **Title VIII: Registration and Voting Statistics** – Directed the Census Bureau to collect registration and voting statistics based on race, color and national origin, but provided that individuals could not be compelled to disclose such information.
- **Title IX: Intervention and Removal of Cases** – Made reviewable in high federal courts the action of federal district courts in remanding a civil rights case to state court and authorized the Attorney General to intervene in certain private suits.
- **Title X: Community Relations Service** – Created the Service to aid communities in resolving disputes relating to discriminatory practices based on race, color or national origin.
Focusing on Title VII of the Act

Prior to the passing of the Civil Rights Act, an employer could legally reject a job applicant because of his/her race, religion, sex or national origin. Title VII of the Act made employment discrimination on the basis of one’s race, religion, sex, national origin and color illegal. All companies with 15 or more employees are required to adhere to the rules set forth by Title VII of the Civil Rights Act.

Title VII protects both employees and job applicants in the following ways:

- Employers are prohibited from making hiring decisions based on an applicant’s race, color, religion, sex or national origin. Employers cannot discriminate based on these factors when recruiting job candidates, advertising for a job, or testing applicants.
- Employers cannot decide whether or not to promote or fire a worker based on the listed factors. S/he also is prohibited from using such information when classifying or assigning workers.
- Employers are prohibited from using information on an employee’s race, color, religion, sex or national origin to determine his/her pay, fringe benefits, retirement plans or disability leave.
- Employers are prohibited from harassing employees based on race, color, religion, sex or national origin.

Employees wishing to make a complaint regarding workplace discrimination, or discrimination during the hiring process should view the EEOC website and read the rules for filing a charge of employment discrimination.

In 2012, the EEOC received over 99,000 individual charges of workplace discrimination. 33.7 percent of total charges were race-based; 30.5 percent of total charges were sex-based; 10.9 percent of the charges were national origin-based.

Summary

This article provides a brief introduction to the Civil Rights Act of 1964, one of the most prominent pieces of civil rights legislation in the US. The article summarizes each Title of the Act and focuses on Title VII, which prohibits employment discrimination on the basis of race, religion, national origin, sex and color.
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Civil Rights Act of 1964 (IV.A.c.i.)
Americans with Disabilities Act

The Americans with Disabilities Act (ADA) represents the most comprehensive civil rights legislation adopted to prohibit discrimination against people with disabilities. Public and private businesses, state and local government agencies, private entities offering public accommodations and services, transportation and utilities are required to comply with the law, which was signed in 1990.

A closer look at the Act

The Act extends civil rights protections to individuals with physical or mental disabilities in the following areas:

- Employment (Title I)
- Public transportation and state and local government services (Title II)
- Public accommodations (Title III)
- Telecommunications (Title IV)
- Miscellaneous (Title V)

Title I of the Act prohibits private employers, state and local governments, employment agencies and labor unions from discriminating against qualified individuals with disabilities in job application procedures, hiring, firing, advancement, compensation, job training, and other terms, conditions and privileges of employment. The ADA covers employers with fifteen or more employees, including state and local governments. It also applies to employment agencies and labor organizations.

According to the ADA, an individual with a disability is a person who:

- Has a physical or mental impairment that substantially limits one or more major life activities
- Has a record of such an impairment, or
- Is regarded as having such an impairment.

A qualified employee or applicant with a disability is an individual who, with or without reasonable accommodation, can perform the essential functions of the job in question. According to the ADA, “reasonable accommodation” may include (but is not limited to):

- Making existing facilities used by employees readily accessible to and usable by persons with disabilities.
- Job restructuring, modifying work schedules, reassignment to a vacant position.
• Acquiring or modifying equipment or devices; adjusting or modifying examinations, training materials or policies; and providing qualified readers or interpreters.

Employers are required to make reasonable accommodations to the known disabilities of a qualified applicant or employee if it would not impose an “undue hardship” on the operation of the employer’s business. Reasonable accommodations are adjustments or modifications provided by an employer to enable people with disabilities to enjoy equal employment opportunities.

Enforcement & Promotion of the ADA

The following federal agencies are responsible for enforcing/promoting the ADA:

• Department of Labor – Provides publications and other technical assistance on the basic requirements of the ADA. It does not enforce any part of the law.
• Equal Employment Opportunity Commission (EEOC) – Enforces regulations covering employment.
• Department of Transportation – Enforces regulations governing transit.
• Federal Communications Commission (FCC) – Enforces regulations covering telecommunication services.
• Department of Justice – Enforces regulations governing public accommodations and state and local government services.
• Architectural and Transportation Barriers Compliance Board (ATBCB, or Access Board) – Issues guidelines to ensure that buildings, facilities and transit vehicles are accessible and usable by people with disabilities.

Encouraging Employment

The Internal Revenue Code (IRC) includes several provisions which help make businesses more accessible to people with disabilities. The most significant tax incentives are outlined below:

1. Small Business Tax Credit – Small businesses with <$1,000,000 in revenue, or 30 or fewer full-time employees may take a tax credit of up to $5,000/year for the cost of providing reasonable accommodations (e.g. sign language interpreters, readers, materials in alternative format, the purchase of adaptive equipment, the modification of existing equipment, or the removal of architectural barriers.}
2. **Work Opportunity Tax Credit** – Employers who hire certain targeted low-income groups (e.g. individuals referred from vocational rehabilitation agencies, individuals receiving Supplementary Security Income (SSI)) may be eligible for an annual tax credit of up to $2,400 for each qualifying employee who works at least 400 hours during the tax year. Additionally, a maximum credit of $1,200 may be available for each qualifying summer youth employee.

3. **Architectural/Transportation Tax Deduction** – This annual deduction of up to $15,000 is available to any business for the cost of removing barriers for people with disabilities.

**Summary**

This article takes a look at the Americans with Disabilities Act (ADA), which prohibits private employers, state and local governments, employment agencies and labor unions from discriminating against qualified individuals with disabilities in job application procedures, hiring, firing, advancement, compensation, job training, and other terms, conditions and privileges of employment.

**CIPP Exam Preparation**

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Americans with Disabilities Act (IV.A.c.ii.)
Genetic Information Nondiscrimination Act (GINA)

The Genetic Information Nondiscrimination Act (GINA) was signed in 2008. The GINA protects Americans from being discriminated on the basis of differences in their DNA which may affect their health.

What is genetic discrimination?

Genetic discrimination takes place when people are treated differently because they have a gene mutation that causes or increases the risk of an inherited disorder. People who undergo genetic testing may be at risk for such discrimination. For instance, a health insurer may refuse to give coverage to a woman who has a DNA difference that raises her odds of getting breast cancer. Employers may use DNA information to decide whether to hire or fire workers.

“Advances in medical science are bringing us closer toward understanding the genetic underpinnings of disease, which could pave the way for new treatments or therapies. But a growing number of experts fear this progress could have serious unintended consequences for the public, allowing insurers and employers to use that information to deny coverage and benefits,” writes health columnist Carly Weeks.

Fear of discrimination may discourage individuals from making decisions and choices, which may be in their best interest. For instance, a father may not undergo genetic testing for fear of consequences to his career or the loss of insurance for his family, despite the knowledge that early therapy could improve his health and longevity.

The Genetic Information Nondiscrimination Act is a Necessity

The GINA is a piece of federal legislation that protects Americans from being treated unfairly because of differences in their DNA that may affect their health. The Act prevents discrimination from health insurers and employers. It was a long-awaited law, which had been debated in Congress for 13 years.

Protection from genetic discrimination is necessary for the following major reasons:

- Genetic discrimination is real and growing
- Genetic discrimination is unjust
- Genetic discrimination is a public concern
- Fear of genetic discrimination prevents positive uses of genetic information

Federal nondiscrimination legislation was proposed as a solution to actual cases of genetic discrimination as well as to prevent fears of potential genetic discrimination, which was seen as...
a major barrier to participation in testing and clinical trials. On the state level, legislatures responded to concerns by providing various levels of protection. The Genetic Information Nondiscrimination Act (GINA) provides a federal floor for protection.

**Nondiscrimination in Health Insurance & Employment**

GINA covers genetic information of an individual and the genetic information of family members (e.g. in determining family health history of disease). GINA does not cover an individual’s manifested disease or condition – a condition from which an individual is experiencing symptoms, being treated for, or that has been diagnosed.

Title I of the GINA covers genetic nondiscrimination in health insurance. It outlines unlawful practices for health insurers in the use of genetic information. GINA prohibits the following:

- Health insurers are not permitted to require individuals to provide their genetic information or that of a family member for eligibility, coverage, underwriting or premium-setting decisions.
- Health insurers may not use genetic information, either collected with intent, or incidentally, to make enrollment or coverage decisions.
- Health insurers may not request or require that an individual or an individual’s family member undergo a genetic test.
- In the Medicare supplemental policy and individual health insurance markets, genetic information cannot be used as a preexisting condition.

Title II of the GINA outlines unlawful activities for an employer, employment agency, labor organization, or training program in the use of genetic information. GINA prohibits the following:

- An employer may not use genetic information in making decisions regarding hiring, promotion, terms or conditions, privileges of employment, compensation, or termination.
- An employer, employment agency, labor organization, or training program may not limit, segregate, or classify an employee or member, or deprive that employee or member of employment opportunities, on the basis of genetic information.
- An employer, employment agency, labor organization, or training program may not request, require, or purchase genetic information of the individual or a family member of the individual, except in rare cases.
- An employer, employment agency, labor organization, or training program may not fail or refuse to refer an individual for employment on the basis of genetic information, nor may the agency, labor organization, or training program attempt to cause an employer to discriminate against an individual on the basis of genetic information.
- An employer, employment agency, labor organization, or joint labor-management committee may not use genetic information in making decisions regarding admission to or employment in any program for apprenticeship or training and retraining, including on-the-job training.
A labor organization may not exclude or expel from membership, or otherwise discriminate against, an individual because of genetic information.

Summary

This article introduces the Genetic Information Nondiscrimination Act (GINA), which was signed in 2008. GINA protects Americans from discrimination based on differences in DNA which may affect their health. It prevents discrimination from health insurers (Title I) and employers (Title II).

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Genetic Information Nondiscrimination Act (IV.A.c.iii.)
Employee Background Screening Basics

Background checks are widely used in hiring and promotion decisions. Job applicants and existing employees and volunteers may be asked to submit background checks. For certain positions, screening may actually be required by state or federal law. Current concerns regarding security and safety have significantly increased the number of employment background checks conducted. This article takes a look at why background checks are conducted, as well as privacy concerns around the issue.

Why do employers conduct background checks?

Employers may check their current and potential employees for a number of reasons. Here are a few of the most common reasons:

- Avoid negligent hiring lawsuits – the threat of liability is concern enough for many employers.
- Child abuse and child abduction reports have resulted in state laws requiring criminal background checks for anyone who works with children.
- Terrorist acts of 9/11 have increased security and identity-verification strategies by employers.
- Corporate scandals of 2002 have resulted in higher scrutiny for corporate executives, officers and directors.
- Common reports of false or inflated information provided by job applicants.
- Federal and state laws require background checks for certain jobs (e.g. anyone who works with children, the elderly, or the disabled). State and federal government jobs may also require a background check and investigation for a security clearance.
- Increasing availability of personal data on computer databases.

Most employees and applicants are unconcerned with background investigations, however, it can be a worry that an investigator may uncover some information about someone’s personal history that may not be relevant to the job. There is also the possibility that background reports may be taken out of context, or contain incorrect information.
What does a background check include?

Background reports can be as simple as a verification of an applicant’s Social Security Number (SSN), or as complicated as a detailed account of the potential employee’s history and acquaintances. Employers have also been known to search social networking sites for applicants’ profiles.

Some information that might be included in a background check include:

- Driving records
- Vehicle registration
- Credit records
- Criminal records
- SSNs
- Education records
- Court records
- Workers’ compensation
- Bankruptcy
- Character references
- Neighbor interviews
- Medical records
- Property ownership
- State licensing records
- Past employers
- Incarceration records
- Sex offender lists
- Personal references

The federal Fair Credit Reporting Act (FCRA) sets national standards for employment screening. The Act applies to background checks performed by outside companies, known as consumer reporting agencies (CRAs). The Act does not apply in situations where the employer conducts background checks in-house.
Under the FCRA, a background check is known as a “consumer report,” the same name given to a credit report, thus the same limits of disclosure apply. According to the FCRA, the following information cannot be reported:

- Bankruptcies after 10 years
- Civil suits, civil judgments and records of arrest, from date of entry, after seven years
- Paid tax liens after seven years
- Accounts placed for collection after seven years
- Any other negative information (except criminal convictions) after seven years.

It's important to note that the above reporting restrictions do not apply to jobs with an annual salary of $75,000 or more per year. Also, the FCRA does not prohibit an employer from asking questions in an employment application about things that should not be reported.

Credit Reports & the FCRA

Under the Fair Credit Reporting Act (FCRA), businesses must obtain an employee's written consent before seeking an employee's credit report. If an employer chooses not to hire or promote someone based on the information in the credit report, it is necessary to provide a copy of the report and let the applicant know of his/her right to challenge the report under the FCRA.

The main purposes of the FCRA are to protect consumers from identity theft and from harm caused by CRAs and the sources that provide data to those agencies. Under the FCRA, all employment background companies constitute CRAs and are obligated to comply with the FCRA, as it pertains to employment.

Employers must take the following steps to ensure compliance with the FCRA:

1. Fully inform the applicant of the nature and scope of the check being done and the fact that the information will be used to make employment decisions. Note that this notice must be in a document separate to the job application. After receiving the disclosure, the applicant has to provide a written release prior to the commencement of the background check.

2. In circumstances that employers would take “adverse action” (i.e. refusing employment or dismissing an applicant) based in whole or in part on a report provided by a CRA, employers must provide applicants/employees with a) Notification that a decision is pending based on the report, known as the Pre-Adverse Action Letter; b) A copy of the report and c) A copy of A Summary of Your Rights Under the Fair Credit Reporting Act.

3. After the decision to take adverse action has been made, employers must provide the following to the applicant/employee: a) Notice that the adverse action was taken; b) The name, address and phone number of the CRA that compiled the report, along with notification that the CRA did not make the hiring decision and cannot provide the specific reasons why the adverse action was taken; c) Notice that the applicant has the right to
obtain another copy of his/her report within 60 days, and that he/she further has the right to dispute any incomplete or inaccurate information furnished by the CRA.

Summary

Job applicants and existing employees and volunteers may be asked to submit background checks for a wide variety of reasons. This article takes a look at why background checks are conducted, the types of information that can and cannot be included in background checks and the regulations around employee/applicant background checks. The article explores how the Fair Credit Reporting Act (FCRA) determines what can and cannot be disclosed, as well as the procedures for employers conducting such checks.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Employee background screening (IV.B.a.)
- Screening requirements under FCRA (IV.B.a.i.)
Employee Background Screening: A closer look at requirements and methods

Background checks are widely used in hiring and promotion decisions. Job applicants and existing employees and volunteers may be asked to submit background checks. For certain positions, screening may actually be required by state or federal law. This article develops on background screening practices and regulations introduced in a previous article.

Sources of Information

Employers may consult a wide variety of information sources as part of a pre-employment check, including:

- **Credit reports** – Under the [Fair Credit Reporting Act](https://www.consumerfinance.gov/), businesses are required to obtain an employee’s written consent before seeking an employee’s credit report.

- **Criminal records** - State law determines the extent to which a private employer may consider an applicant’s criminal history in making employment decisions. Federal law also gives the [Federal Bureau of Investigation](https://www.fbi.gov) (FBI) the authority to conduct a criminal history record check for non-criminal justice purposes. The FBI can exchange criminal history record information with officials of state and local governments for employment, licensing, which includes volunteers, and other similar non-criminal justice purposes.

- **Lie detector tests** – The [Employee Polygraph Protection Act](https://www.dol.gov/esa/policy/employeepolygraphact.html) (EPPA) prohibits most employers from using lie detector tests, for pre-employment screening or during the course of employment. However, the EPPA includes a list of exceptions that apply to businesses that provide armored car services, alarm or guard services, or those that manufacture, distribute, or dispense pharmaceuticals. Although there is no federal law prohibiting use of a written honesty test on job applicants, these tests frequently violate federal and state laws that protect against discrimination and privacy violations.

- **Medical records** – Under the [Americans with Disabilities Act](https://www.ada.gov) (ADA), employers cannot discriminate based on a physical or mental impairment or request an employee’s medical records. However, businesses are permitted to inquire about an applicant’s ability to perform specific job duties. Some states also have stricter laws protecting the confidentiality of medical records.

- **Bankruptcies** – Bankruptcies are a matter of public record and may appear on an individual’s credit report. The federal [Bankruptcy Act](https://www.legis.state.us/110/bankruptcy Act) prohibits employers from discriminating against applicants because they have filed for bankruptcy.

- **Military service** – These records may be released only under limited circumstances, and consent is normally required. The military is permitted to disclose name, rank, salary, duty assignments, awards and duty status without the service member’s consent.

- **School records** – Under the [Family Educational Rights and Privacy Act](https://www.ed.gov) (FERPA) and other similar state laws, educational records such as transcripts, recommendations and financial information are confidential and will not be released by the school without a student’s consent.
• Worker’s compensation records – Worker’s compensation appeals are a matter of public record. Information from appeals may be used in a hiring decision, if the employer can show the applicant’s injury might interfere with his/her ability to perform required duties.
• Psychological and personality testing – Such tests may assess individuals’ general aptitude, intelligence and personality.

Blind Spots

Under the Fair Credit Reporting Act (FCRA), background checking agencies are required to maintain procedures to ensure the accuracy of the information they report about the consumer. The FCRA regulates what can and cannot be included on reports, however there are two major loopholes. The first is if the employer does not use a third-party screening company, but opts to conduct the background check itself, it is not subject to the notice and consent provisions of the FCRA.

Secondly, the employer might tell the rejected applicant that the adverse decision was not based on the contents of the background investigation, but that the job pool was so exceptional that it made its hiring decision based on the fact that there were individuals more qualified than the applicant.

In both situations, the applicant would not have the ability to obtain a copy of the background check to find out what negative information it contained.

Summary

Job applicants and existing employees and volunteers may be asked to submit background checks for a wide variety of reasons. This article introduces the various methods and sources of information for background checks and pre-employment screening. While the Fair Credit Reporting Act (FCRA) regulates the type of information that may be included on background reports, there are two major loopholes that are commonly used in the screening process.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

• Employee background screening (IV.B.a.)
• Screening requirements under FCRA (IV.B.a.i.)
• Screening methods (IV.B.a.ii.1. – IV.B.a.ii.4.)
Psychological and Personality Testing in Employment Screening

Most companies realize the value in using psychological tests as part of the employee selection and promotion process. Testing can often bring objectivity and validity to the recruitment process; however employers who administer tests in the hiring or promotion processes must be aware of the legal obstacles and privacy risks involved.

Why use psychological and personality tests?

Pre-employment testing can be useful in reducing the time HR personnel spend interviewing applicants by automatically eliminating a percentage of the applicant pool. Psychological tests can also be helpful in determining an employee or applicant’s honesty and integrity. Integrity tests are written tests that predict whether an employee will engage in theft, as well as reflect their general trustworthiness and dependability.

Risks Involved

There are significant legal implications in administering psychological tests to employees and applicants. For instance, the 2005 case *Karraker v. Rent-A-Center Inc.* shows the risks associated with psychological testing. The case held that administering certain psychological tests to employees violates the *Americans with Disabilities Act* (ADA). The court found that the employer’s use of the *Minnesota Multiphasic Personality Inventory* (MMPI) as part of its testing process for managers violated the ADA. The MMPI is a test for adult psychopathology and can be used by medical professionals to diagnose some psychiatric disorders.

Furthermore, employers could face lawsuits from employees who believe that confidentiality laws were violated in the handling of their test results. Employers have an obligation to maintain confidentiality of the test answers and to avoid providing information that could be deemed confidential without the employee’s consent.

For these reasons, certain states have enacted laws prohibiting the psychological testing of employees. Other states have stringent statutes banning the use of lie-detector testing. Massachusetts broadened the scope of its polygraph-protection law to prevent employers from using written examinations used to render a diagnostic opinion regarding an individual’s honesty. California and Rhode Island laws require that honesty and integrity exams cannot be the primary basis for making hiring, firing or promotion decisions.
Best Practices

It should be clear that use of psychological or personality testing of current or potential employees represents a risk for litigation. Employers still considering such tests should consider the following precautions and practices:

- Never use psychological or personality tests as the sole criterion for hiring or promotion decisions.
- Avoid using tests that require analysis by a psychologist, psychiatrist or social worker.
- Review existing tests to ensure they do not include a psychological diagnostic component. Ensure the test does not contribute to a finding of a particular mental impairment or psychological disorder.
- Ensure the test is statistically valid, reliable and devoid of cultural and ethnic bias.
- Use tests that are job-related and of a business necessity.
- Administer the test in a standardized fashion that ensures that all job applicants or employees are assessed in the same way.
- Monitor the test results to ensure that there is not a disparate impact on certain groups.
- Take active steps to ensure the confidentiality of test responses.
- Monitor workplace statistics on attrition, theft, turnover and production to determine whether the use of these tests has resulted in a reduction of identified counterproductive or undesirable behaviors.
- Consult a lawyer or advisor with expertise in the area of employment screening before implementing testing activities. At the very least, an employer must comply with federal requirements, as well as any additional requirements imposed by the state where the test is being administered.

Common Tests

Psychological and personality tests assess an individual’s general aptitude, intelligence and personality. Some common test types are introduced below.

- **Myers-Briggs Type Indicator** – This testing system is generally used by private companies and federal government agencies. It organizes personality data along four scales of opposing characteristics. Companies use this test to match employees to the right jobs, improve organizational communications and design training programs.
- **IPIP-NEO Personality Test** – This measures an employee’s personality of five broad personality categories and 30 sub-categories. Organizations often use this test to evaluate an employee’s ability to get along in a multicultural setting.
• **Kolbe Index** – This is based on the notion that an employee’s problem-solving abilities are stable and independent of intelligence, personality and education. Employees are asked to answer several multiple-choice questions based on problem-solving scenarios.

**Summary**

Psychological and personality testing can often bring objectivity and validity to the recruitment process; however employers who administer tests in the hiring or promotion processes must be aware of the legal obstacles and privacy risks involved. This article examines some of the risks involved in testing and introduces best practices for employers interested in conducting such tests for current or future employees.

**CIPP Exam Preparation**

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Employee background screening (IV.B.a.)
- Screening methods – personality and psychological evaluations (IV.B.a.ii.1.)
Problems with Background Screening in the Workplace

As we’ve discussed in previous articles, employee background checks are required in a number of industries to ensure public safety and security. Background checks are being conducted more frequently than ever before. Indeed, according to a 2012 study conducted by the National Consumer Law Center, about 73 percent of employers conduct criminal background checks for all potential applicants. However, evidence indicates that professional background screening companies routinely make mistakes, often with serious consequences for job seekers.

The Industry

Companies providing a background check service are part of a growing industry. The industry is made up of large national corporations, as well as numerous smaller local and regional companies providing criminal record information to employers. According to a BusinessWeek article:

“Background screening has become a highly profitable corner of the HR world. At the screening division of First Advantage (FADV), based in Poway, Calif., profits soared 47% last year, to $29 million; revenue grew 20%, to $233 million. HireRight (HIRE), based in Irvine, Calif., reported that earnings jumped 44%, to $9 million, last year on revenues of $69 million. To grab a piece of this growing market, Reed Elsevier Group (RUK), the Anglo-Dutch information provider, agreed to acquire ChoicePoint for $4.1 billion in February – at a 50% premium to its stock price.”

There are currently no licensing requirements to become a background checking agency and no system for registration exists. Essentially, anyone with a computer, internet connection and access to records can start a background screening business.

Accuracy is an Issue

Attorneys and community organizations that work with consumers with problematic background reports say that they often see background reports that:

- Mismatch the subject of the report with another person
- Reveal sealed or expunged information
- Omit information about how the case was disposed or resolved
- Contain misleading information
- Mischaracterize the seriousness of the offense report

Mismatched reports are an extremely common problem with criminal background reports. These contain the criminal history of a person other than the subject of the report, and are mainly the result of unsophisticated matching criteria. Biometric identification systems help to reduce the

CIPP/US Prep Guide
chances of incorrectly connecting someone to the criminal record of another. Private background check companies typically match information in their databases using non-biometric information (e.g. name and birth date).

Another problem within the screening industry involves the common practice of subcontracting out the search for criminal records. However, the subcontracting does not stop with one vendor, but continues as the vendors themselves subcontract the work to other vendors. This practice of sub-sub-sub-contracting drastically reduces accountability and increases the likelihood of erroneous information. The majority of background check agencies do not demand stringent quality controls over the information provided by vendors.

One of the most damaging mistakes an agency can make is to reveal sealed or expunged data. The information revealed in such records is nearly impossible to dispute with the employer. If the agency has mixed the job applicant’s file with another person, the applicant can argue it was not him/her. In the case of a sealed conviction, the applicant cannot claim that the accusation is false, but merely that the employer should not know about it.

Background check companies might also omit final disposition data. This means that the companies would report the fact that charges were filed, but not whether the person was convicted. Because of this omission, people who have been exonerated of the charges against, or had the charges dropped or reduced, appear to have pending criminal complaints against them.

Certain screening agencies will dedicate considerable space on their reports to tout the jurisdictions they search, but will leave significantly less space to the results of those searches. Even more worrisome is that background screening agencies have been known to report single arrests or incidents multiple times. Screening agencies will also attempt to subvert the time limits for information in the FCRA by telling potential employers that the company has information that it could not share.

Advocates across the US report that they often see mistakes on commercial background reports, due to a fundamental misunderstanding of how states report and classify information. In particular, commercial background screening agencies repeatedly misreport the level or classification of the offense. Additionally they rarely know what to do with offenses that are classified as less than a misdemeanor or are non-criminal offenses (e.g. traffic tickets).
Recommendations

The National Consumer Law Center recommends the Consumer Financial Protection Bureau (CFPB) use its rulemaking authority under the Fair Credit Reporting Act (FCRA) to:

- Require mandatory measures to ensure greater accuracy.
- Define how long an employer has to wait in between sending an initial notice and taking an adverse action (i.e. rejecting an applicant or terminating an employee).
- Require registration of consumer reporting agencies.

The Federal Trade Commission (FTC) could also enforce the FCRA in the following ways:

- Investigate major commercial background screening companies for common FCRA violations.
- Investigate major, nationwide employers for compliance with FCRA requirements imposed on users of consumer reports for employment purposes.

Summary

Companies providing a background check service are part of a quickly growing industry, however, errors in reporting can have serious and long-lasting consequences on job seekers. Attorneys and community organizations that work with consumers with problematic background reports say that agencies often produce reports that contain inaccurate information. This article takes a look at some of the most common problems within the background screening industry.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Employee background screening (IV.B.a.)
- Screening requirements under FCRA (IV.B.a.i.)
- Screening methods (IV.B.a.ii.1. – IV.B.a.ii.4.)
Social Media Analytics in Employee Recruitment

A study published in the *Journal of Applied Social Psychology* found that social network profiles of job applicants were surprisingly good predictors of how well they might fit into an organization. Researchers reported that they could accurately assess, based on an analysis of the Facebook posts of 500 people, how a job candidate would rank in the “Big 5” personality traits: 1) Openness to experience; 2) Conscientiousness; 3) Extroversion; 4) Agreeableness; and 5) Neuroticism. It was suggested that if social networks can provide an evaluation of how well an individual will do in a particular job, then employers should use such platforms as the first stage of screening in the interview process.

Social Media Trend

A major part of the job recruitment process has already moved online. These days, employers are looking for potential candidates via sites like LinkedIn, or tracking applicants through tools like Monster or Career Builder. Social networks can also help employers get in touch with a different pool of candidates, not just the ones that apply for the job.

Studies on social media analytics have shown that almost 40 percent of technology industry companies check their potential employees’ profiles on social media sites. Mads Christensen, Network Director at Eurocom Worldwide, says “The 21st century human is learning that every action leaves an indelible digital trail. In the years ahead many of us will be challenged by what we are making public in various social forums today.”

What about privacy?

Using social media analytics as a recruitment tool also brings up concerns about user privacy. Candidates may feel that companies are unjustifiably basing their decisions on a person’s social media activities. Job seekers and privacy advocates often argue that personal life should not be confused with work life and as such, social media profiles should not be used as part of the decision-making process in recruitment.

According to Chirag Nangia, CEO of Reppify, a San Francisco-based business that uses integrated social media data to help companies find the right people:

“Employers have to be constantly aware of the types of information they are restricted from using in the selection process. However, because doing a web search on a candidate reveals many types of information, including information deemed ‘Protected Class’ (race, gender, etc.), it can be potentially dangerous to manually assess candidates’ social media properties. Aside from being restricted, the process is time consuming and cumbersome to use when comparing across candidates. For job seekers, it opens up questions around what they should or should not post to their own closed network of friends and family, which we believe is setting the wrong precedent.”
Another concern is that employers might be too dependent on social media information when making hiring decisions. According to the 2012 annual technology market survey conducted by Eurocom Worldwide, almost one in five technology industry executives say that a candidate’s social media profile has caused them not to hire a person. This survey is the first evidence that prospective job candidates are actually being rejected because of their profiles.

Proponents of the practice argue that social media analytics data should not be used on their own, rather as part of the overall recruitment process, together with face-to-face interviews, tests, background checks and other proven methods of determining a candidate’s likely performance in a job and his/her organizational fit.

Summary

This article explores how social media analytics has impacted the job recruitment and applicant assessment process. 40 percent of tech companies have reported that they use social media profiles in their hiring process, while 20 percent of these companies have admitted that a candidate’s social media profile has actually caused them not to hire a person.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Employee background screening – social media (IV.B.a.ii.4.)
Employee Monitoring & Privacy Expectations

Technology has allowed employees to enjoy increased autonomy and flexibility with things like telecommuting and mobile working. However the same tools have also been used to facilitate the intrusion of professional life into the personal sphere and sometimes the intrusion of the employer into the private lives of its employees.

Monitoring & Privacy in the US

US employers engage in a variety of work-related monitoring practices for a range of legitimate business purposes. Employees in the US tend to have minimal expectations of privacy in the workplace, while employers usually destroy any remaining limited expectations through notices and warnings regarding monitoring in employee handbooks, computer log-in screens, electronic systems use policies and privacy statements.

Employers in the US argue that there are many good business reasons to electronically monitor employees in the workplace. Here are some of the major reasons for implementing monitoring practices:

- Monitor employee productivity in the workplace.
- Maximize productive use of the employer’s computer system when employees use computers on the job.
- Monitor employee compliance with employer workplace policies related to use of its computer systems, email systems and internet access.
- Investigate complaints of employee misconduct, including harassment and discrimination complaints.
- Prevent or detect industrial espionage (e.g. theft of trade secrets and other proprietary information; copyright infringement; patent infringement; trademark infringement).
- Prevent or respond to unauthorized access to the employer’s computer systems, including access by computer hackers.
- Protect computer networks from being overloaded by large downloadable files.
- Prevent or detect unauthorized utilization of the employer’s computer systems for criminal activities and terrorism.
- Help prepare the employer’s defense to lawsuits or administrative complaints such as those brought by employees related to discrimination, harassment, discipline, or termination of employment.
- Respond to discovery requests in litigation related to electronic evidence.
A “reasonable expectation” of privacy

As employers compensate employees to perform their jobs, the courts have traditionally granted employers wide latitude to monitor their employees’ work performance and productivity, provided that such monitoring does not violate an employee’s reasonable expectation of privacy. Courts usually act deferentially, even when employers engage in electronic surveillance (e.g. monitoring phone lines, email accounts and internet access), as long as the employer has disclosed its monitoring policy to its employees.

State & Federal Regulations

Before employing any form of electronic monitoring, organizations should be aware of two important pieces of federal legislation:

- Electronic Communications Privacy Act of 1986 (ECPA)
- National Labor Relations Act (NLRA)

The ECPA restricts employers from monitoring employee telephone calls or emails when employees have a reasonable expectation of privacy. Organizations may intercept communications when there is actual or implied member consent. Simply notifying members that monitoring takes place can constitute consent.

The NLRA is known for guaranteeing workers the right to join unions without fear of management reprisal, however the Act might have some relevance to internet and network monitoring. The National Labor Relations Board (NLRB) has reported that a company’s computer network is a “work area.” Any rules prohibiting all non-business use of email on a company’s network could therefore be considered unlawful under the NLRA. Organizations can also be in violation of the NLRA when the monitoring of members is found to selectively punish labor organizing activities.

Some states have enacted laws requiring organizations to give notice to members before engaging in electronic monitoring activities. It’s important to note, however, that even in states with legislation covering this issue, organizations wishing to monitor their members are not necessarily restricted. Most state laws covering this issue attempt to impose regulations on the frequency and extent of notification.
ILO’s Code of Practice

The International Labor Organization (ILO) is active in the debate surrounding internet and network monitoring. It has developed a code of practice that may be used as a guideline for other organizations developing their own privacy and acceptable use policies. The Code specifies that employees’ data should be collected and used consistently with Fair Information Practices (FIPs).

These practices include:

- **Notice**: Data collectors must disclose their information practices before collecting information from consumers.
- **Choice**: Consumers must be given options with respect to how personal information collected from them may be used for purposes beyond those for which the information was provided.
- **Access**: Consumers should be able to view and contest the accuracy and completeness of data collected about them.
- **Security**: Data collectors must take reasonable steps to assure that the information collected from consumers is accurate and secure from unauthorized use.

Summary

US employers engage in a variety of work-related monitoring practices for a range of legitimate business purposes. This article introduces the topic of workplace monitoring in a US context. It also provides an overview of state and federal legislation covering workplace monitoring activities and discusses the International Labor Organization’s (ILO’s) code of practice regarding employee monitoring.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Employee monitoring (IV.B.b.)
CIPP Applied – We’re not Facebook friends! Employee screening through social media sites

On Monday, April 9, 2012, Maryland became the first state in the US to officially ban employers from requesting access to the social media accounts of current employees and job applicants. This is the culmination of a controversial employee screening practice which involves employers getting potential candidates’ Facebook usernames and passwords to assess their suitability for hire. While many companies would like to take a close look at potential employees to ensure that they are not involved in any activity that would be harmful to the company and learn more about the person’s attitudes and preferences, accessing their personal social media accounts represents a boundary that many feel should be respected.

Screening Practice

It’s become a common practice for certain employers to request their current and potential employees to hand over their Facebook login information. Sometimes, Facebook credentials are even a requirement to secure a job. Employers who do this believe that it’s a great way to research job candidates. However, the screening practice is generally limited to browsing their wall, photos and posts from an outsider perspective. Forcing employees to hand over passwords allows employers to view some of their most private online data, in which they can access information that the user had intended to control through privacy settings.

Observers have warned that this practice could raise problems for employers as well as their employees. Conducting an unrestrained search of someone’s Facebook account could reveal information previously unknown to the employer. If any of this information ends up causing the employer to choose not to hire a candidate, and the information happened to involve race, religion or sexual orientation, the employer might become involved in a serious discrimination lawsuit.

Maryland’s New Law

On April 9, 2012, Maryland’s General Assembly passed the bill prohibiting employers from asking current and prospective employees for their usernames and passwords to social media sites, including Facebook and Twitter. The bill was passed unanimously in the Senate and by a wide margin in the house. Lawmakers successfully reconciled the bills ahead of the end of the legislative session on April 9. It is currently awaiting signature from Governor Martin O’Malley, whose stance on the bill was still unclear.
This is the first bill of its kind in the country, bringing even more attention to the controversial practice. According to Melissa Goemann, legislative director of the American Civil Liberties Union of Maryland, “We just think this is a really positive development, because the technology for social media is expanding every year, and we think this sets a really good precedent for limiting how much your privacy can be exposed when you use these mediums.”

Not Alone

Maryland is not alone with their concerns about this privacy-invasive practice. Similar piece of legislation to Maryland’s new bill have been introduced in Illinois and California. In late March 2012, Richard Blumenthal (D-CT) announced he was drafting legislation to prohibit employers from demanding Facebook login information of prospective employees. He joined Chuck Schumer (D-NY) to request that the Department of Justice look into the potential illegality of the practice.

Blumenthal commented that he was “deeply troubled by the practices that seem to be spreading voraciously around the country,” and that the password requests are an “unreasonable invasion of privacy.”

Blumenthal’s proposed bill would not make it illegal to use information gained from public Facebook activity. This means that employers could still take a look at anything a regular Facebook browser could see. The bill just prohibits requesting for their employees’ passwords.

On its Passwords and Privacy blog, Facebook spoke out against the practice, deeming it both “distressing,” “alarming” and “potentially exposes the employer… to unanticipated legal liability.” The blog went on to establish that no one should be forced to share private information in order to get a job, and that the trend of soliciting employees’ passwords “undermines the privacy expectations and the security of both the user and the user’s friends.”

Summary

In recent months, incidents of employers requesting potential new hires’ social media usernames and passwords have made headlines and sparked outrage in the privacy rights community. The practice of accessing personal social media accounts gives employers insight into what their employees may be like and if they would be a good fit with the company, however, this also means that they can take a look at information that the individual may not want to be made private. The article discusses the practice, as well as Maryland’s bill prohibiting employers from doing so. The bill, passed April 9, 2012, was the first of its kind in the United States.
CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, as well as the Certification Foundation Course (Foundations), a privacy professional should be comfortable with topics related to this post, including:

- Employee background screening – social media (IV.B.a.ii.4.)
End-of-Chapter Review

HR Goals

- Attract and retain talent
- Provide excellent customer service
- Make tools and data available for corporate planning functions
- Manage costs of HR functions

The following tools are available to achieve HR goals:

- Background-check new employees
- Employee monitoring to ensure compliance with laws and regulations
- Centralized HR databases
- Global intranet systems
- Connectivity technology
- Global benefits and compensation program
- Advancement planning
- Data processing vendors
- Outsource benefits, payroll, etc.

However, HR resource management brings high liability potential.

HR & Privacy Issues

1. Before Employment
   - Application/interview process
   - Background check

2. During Employment
   - Skills testing
   - Workplace monitoring
   - Misconduct investigations
3. After Employment

- Termination procedures
- Transition management
- Post-termination claims
- Retention/destruction of documents

**Workplace: US vs. EU**

<table>
<thead>
<tr>
<th>US: focus on employer duties</th>
<th>EU: focus on employee rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security concerns are central</td>
<td>Privacy concerns are central</td>
</tr>
<tr>
<td>Continuous, multi-dimensional employee monitoring is acceptable</td>
<td>Employee monitoring is limited</td>
</tr>
<tr>
<td>Background checks are acceptable and required</td>
<td>Background checks are limited</td>
</tr>
<tr>
<td>Low employee expectations of privacy</td>
<td>High employee expectations of privacy</td>
</tr>
</tbody>
</table>

**US Employee Privacy Protection**

- No unified law applies to employee data.
- Most US labor laws mandate data collection/management practices.
- Federal and state laws may regulate employment and HR data management.
- Federal laws rarely preempt state laws.

Employee data handling practices in the US are regulated by:

- Department of Labor
- EEOC (Equal Employment Opportunity Commission)
- HHS (Department of Health & Human Services)
- State Department of Labor
- National & State Labor Relations Boards

**Occupational Safety and Health Act (OSHA)**

- Assures safe and healthful working conditions for working men and women
- Administered through Dept. of Labor
- Many states have equivalent laws
Anti-Discrimination Laws

These are US Federal laws that limit the information employers are able to collect:

- Equal Pay Act of 1963
- Civil Rights Act of 1964
- Pregnancy Discrimination Act
- Age Discrimination Act of 1967
- Americans with Disabilities Act of 1990
- Genetic Information Nondiscrimination Act of 2008

Employers cannot ask applicants questions regarding:

- Race
- Religion
- National origin/descent
- Marital status (e.g. spouses, relatives, children, dependents)
- Physical characteristics – height and weight can only be asked if it is job-related
- Pregnancy status
- Medical conditions and disabilities – employers can only ask if the applicant can perform the essential functions of the job, with/without a reasonable accommodation
- Citizenship status – cannot ask if the applicant is a US citizen or if they can provide documentation
- Arrests and convictions – can only ask about convictions within the last ten years, as long as they are convictions related to job performances

Benefits Regulations

These are US Federal laws that regulate information handling and employee benefits:

- Health Insurance Portability & Accountability Act (HIPAA)
- Consolidated Omnibus Budget Reconciliation Act (COBRA)
- Employee Retirement Income Security Act (ERISA)
- Family & Medical Leave Act (FMLA)
Data Collection & Record Keeping

These are US Federal laws that impose requirements for data collection and record keeping:

- Fair Credit Reporting Act (FCRA)
- Fair Labor Standards Act (FLSA)
- Occupational Safety & Health Act (OSHA)
- Immigration Reform & Control Act (IRCA)

Employee Photographs

- Employers may not ask applicants to provide photos before hiring.
- Photos may only be requested after hiring for ID purposes.
- Employee consent is preferred before posting photos on websites.
- In the EU, consent is required to handle employee photos.

SSN (Social Security Numbers)

- No law prohibiting collection of SSN before job offer.
- Recommended to delay collection of SSN until after the job offer is made, as security laws and breach notification laws would apply.

Applicant Testing

Three types of employee/applicant testing:

1. **Performance** – assesses reactions to real situations
2. **Projective** – assesses interpretation of ambiguous stimuli
3. **Objective** – based on true/false or multiple choice questions

E.g. cognitive ability testing, honesty/integrity testing, interest inventories
Psychological Testing

- May be viewed as medical exams under the ADA (Americans with Disabilities Act).
- Published results may have consequences under common law torts.
- State laws may prohibit psychological testing.

If employee tests are used, they should:

- Only ask job-related questions
- Not include overly-intrusive questions
- Be professionally designed
- Be administered by trained professionals
- Limit access to results
- Have employee consent to the testing (required in EU; a best practice in US)

Examples: Myers-Briggs Type Indicator: IPIP-NEO Personality Test; Kolbe Index.

Polygraph Tests

- Lie detectors = polygraphs and other devices measuring honesty
- Employee Polygraph Protection Act of 1998 (EPP) generally prohibits requiring or using lie detector tests.
- EPP prohibits taking adverse action against employees refusing to take the test.
- EPP allows polygraphs for some investigations, in certain industries.
- Violations of EPP could lead to fines, private right of action.
- EPP does not preempt state laws.

Drug & Alcohol Tests

There are different types of substance abuse testing in the US:

- Pre-employment screening: Cannot be used to identify legal drug use or past/present addiction to illegal drugs.
- Routine testing: Only if employees are informed at time of hire.
- Reasonable suspicion testing: Acceptable condition of continued employment.
- Post-accident testing: Acceptable condition of continued employment, if there is reasonable suspicion of substance abuse at the time of the accident.
- Random testing: Most problematic. Usually accepted in highly regulated industries, or where critical to public safety/national security. Random testing should be part of a systematic substance testing program.
Genetic Testing

Two types of genetic testing:

1. **Screening** – looking at genetic makeup of individual for certain markers
2. **Monitoring** – periodic testing to identify changes to genetic structure over time

Genetic Information Nondiscrimination Act of 2008:

- Prohibits adverse actions on the basis of genetic testing (e.g. discrimination, refusal to hire)
- Other legal claims can be made under:
  - Americans with Disabilities Act
  - State anti-testing laws
  - Common law torts

Best practices for genetic testing:

- Tests should relate to job performance (e.g. detecting hazardous materials in body)
- Employee consent specific to the test
- Restrict access to test results

Background Checks

- Necessary to avoid liability for negligent hiring practices.
- 170 statutes in 41 US states related to employment-related background checks.
- Also regulated by the FCRA.
- Background checks are often job-specific, but may include:
  - criminal records
  - civil litigation history
  - driving history
  - credit records
  - professional credentials
  - references
  - education transcripts
- Similar to limitations on interview questions, background checks should not include:
  - age
  - race
  - religion
  - national origin
  - arrests
  - health/disability issues
  - pregnancy status
  - marital status
• Search engines or social engineering websites cannot be used for background checks.
• Consumer reports can be used for pre-employment screening or for decision-making regarding promotions.
• Use of consumer reports requires **written consent** of the employee.
• According to the FCRA, if a consumer report is used to make an adverse decision about an applicant/employee, the employer must:
  a) Provide notice and a copy of the consumer report before taking the action.
  b) Provide adverse action notice after taking the action.

**Academic Records**
• Regulated by FERPA (Family Educational Privacy Rights Act)
• Student consent required for everything except directory information

**Motor Vehicle & Driving Records**
• Regulated by DPPA (Driver’s Privacy Protection Act)
• Records may be used for consumer reports, with consent

**Employee Monitoring in the US**
• Reasons for employee monitoring:
  o Risk management (e.g. prevention of workplace violence, hostile environment, theft)
  o Quality control
  o Productivity metrics
  o Public health/safety
  o Corporate compliance
  o Secondary purposes (e.g. performance review, investigations)
• Methods for monitoring:
  o Workplace surveillance
  o Sign-in/log-in records
  o Access controls
  o Automated online monitoring
  o Monitoring of telephone, computer, email, Internet usage
Telephone Monitoring

- Regulated by US Federal Wiretap Act, which allows monitoring for:
  - Business Use – calls in the ordinary course of business
  - Prior Consent – if consent has been obtained prior to monitoring (preferably in writing)
- US Wiretap Act does not preempt state law.

Video Monitoring

- Generally unregulated in US; no federal statute, but state privacy laws.
- Should not be used in sensitive areas (e.g. restrooms, changing rooms).
- Recording audio as well as video is regulated by US Wiretap Act.

Email Monitoring

- Regulated by ECPA (Electronic Communications Privacy Act of 1986), which extends Wiretap Act to electronic communications.
- Exceptions to ECPA:
  1. Owners of the equipment can monitor communications through the equipment.
  2. Monitoring with user consent.

Postal Mail Monitoring

- Federal law prohibits mail interferences, though mail is delivered upon reaching the address.
- State law risk can be reduced if:
  - Employees do not receive personal mail at business address
  - Declining to read mail if it is personal
  - Maintaining the confidentiality of personal information

Employee Monitoring Outside the US

- Employee monitoring is strictly limited.
- Must be proportionate to the practices it is meant to detect/prevent.
- Practices must be disclosed to employees, regulators, unions, etc.
- Results of monitoring are considered highly-sensitive.
- Throughout most of the EU, electronic monitoring of employees is prohibited.
Managing Employee Monitoring

Monitoring policies should include:

- When monitoring takes place
- How the data will be used
- To whom the data will be disclosed
- Procedure for responding to data
- Approval process for special circumstances

Employee Misconduct

Such allegations bring the following concerns:

- Liability for negligence
- Protecting the employee during due process
- Corporate policy compliance
- External obligation compliance
- Documenting misconduct
- Considering the rights of other employees involved

Companies may use third-parties to investigate misconduct claims:

- 1999: Resultant reports are investigative consumer reports and subject to provisions of FCRA (i.e. require written consent, notice to individual).
- 2003: Amendments to exclude investigative reports from FCRA coverage.

Employee Termination

- Reason for termination should be documented.
- Employee access to accounts, devices, company information should be stopped.
- Personal data should be returned.
- Terminated employee has the obligation to maintain confidentiality of company data.

Enforcement Actions

- Negative publicity
- "Voluntary request" for documents from FTC
- Settlement agreements
- Consequences with State Attorneys General
Settlement Terms

Depends on type of conduct, but may include:

- Develop formal security program, in case of a breach
- Make no further misrepresentations
- Privacy controls
- Deletion of inappropriate personal information
- Provide documents to FTC, ongoing notification to FTC
- Consumer restitution

Incident Response

- Legal compliance
- Notification letter
- Actions to address consumer harm
- Appropriate vendor management

Incident response best practices include:

- If notices are sent, everyone should receive them.
- Tri-bureau credit monitoring for lost SSNs.
- ID theft education via FTC.
- Appropriate responses to consumers, media.
- Inform regulators.

International Data Transfers

- US laws do not restrict transfers of personal information (geography-neutral).
- US exporter is responsible for inappropriate use by international data processors.
- Personal information imported into the US may be subject to regulations in the originating country.

Privacy Risk Management

1. Legal obligations
2. Reputation and brand considerations
3. Return on investment
4. Over-compliance costs
CIPP Applied – Proposed bill shows states’ rights sometimes fall to bad federal legislation

In the United States, we’re dependent on the overlapping and sometimes confusing patchwork of legislation and regulations because the US employs sectoral versus comprehensive approach to privacy. This legal patchwork sometimes includes state laws in addition to federal, which most see as simply another hurdle towards doing business in that state. In some cases, related but more stringent laws in the state were already passed. In those situations only minor modifications are needed for state compliance with a newly signed federal statute.

The Federal Trade Commission and State Attorneys General enforce federal and state laws of consumer privacy protection for Unfair or Deceptive Trade Practices (UDTP). One recent example was the State of Maine’s consumer protections, which are more restrictive than the federal laws with respect to cigarette labeling. The State brought suit against a tobacco manufacturer for violating the state’s deceptive trade law, which the manufacturer argued was out of line due to the Federal Cigarette Labeling Act. The Supreme Court decision upheld the State’s right to pass more restrictive legislation, pointing out:

Neither the Labeling Act’s pre-emption provision nor the Federal Trade Commission’s actions in this field pre-empt respondents’ state law fraud claim. Pp. 5–20.

(a) Congress may indicate pre-emptive intent through a statute’s express language or through its structure and purpose. See Jones v. Rath Packing Co., 430 U. S. 519, 525. When the text of an express pre-emption clause is susceptible of more than one plausible reading, courts ordinarily “accept the reading that disfavors pre-emption.”

The rationale in (a) requires express language for a federal law to negate a State’s right to create more restrictive legislation. The first citing by the high court becomes the contentious issue for House Bill H.R. 2221, proposed by Illinois Representative Bobby Rush. The bill tackles several tough interstate commerce issues, placing the FTC in charge of disposal regulations for obsolete or abandoned paper records containing personal information, breach
notifications and verification requirements for information brokers. Section 6 of the so-called Data Accountability and Trust Act includes a provision reading:

(a) …This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State, with respect to those entities covered by the regulations issued pursuant to this Act, that expressly--

requires information security practices and treatment of data in electronic form containing personal information similar to any of those required under section 2; and

requires notification to individuals of a breach of security resulting in unauthorized acquisition of data in electronic form containing personal information.

(b) Additional Preemption-

IN GENERAL- No person other than the Attorney General of a State may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.

This would strike several of the state privacy and notification laws (possibly including California's SB 1386),stripping the State's rights and growing Washington's power. It also bars the State Attorneys General from bringing suit, possibly in an effort to avoid a double jeopardy situation. There are numerous case studies of the FTC and State Attorneys General working hand-in-hand for consumer protection; why this law tries to hamstring the situation is a bit of a mystery.

One more interesting note on Representative Rush’s proposal - the bill also places an encryption exemption on breach notification. As we noted in a recent post on corporate disposal policies, hackers and researchers seem to notice protection missteps and use them to bypass security provisions just like encryption.

The encryption of data in electronic form shall establish a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data. Any such presumption may be rebutted by facts demonstrating that the encryption has been or is reasonably likely to be compromised.

The law has a 10 year lifespan, which should be a decent requirement before the Advanced Encryption Standard (AES), currently the de-facto encryption standard (and as yet to be compromised), ages beyond its effectiveness.

Update: President Obama’s May 20th, 2009 Memorandum on the Subject of Preemption and State's Rights quotes Justice Brandeis saying, "[i]t is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."
CIPP Candidate Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with several topics found in this post including:

- Federal vs. state authority (V.A.)
Driver’s Privacy Protection Act (DPPA)

The Driver’s Privacy Protection Act (DPPA) was enacted in response to a number of crimes resulting from abuse of personal information maintained in Department of Motor Vehicle records systems. Most prominent of these crimes, was the death of actress Rebecca Schaeffer. A private investigator retrieved her home address from the California Department of Motor Vehicles database. The information was the used by her stalker to follow and eventually kill her. The Driver’s Privacy Protection Act helps to prevent such crimes by creating strict rules for the disclosure of an individual’s DMV records.

Scope of the DPPA

The Driver’s Privacy Protection Act is a federal law that regulates agencies controlled on the state level. The Supreme Court Case Reno v. Condon, challenged the Federal government’s authority to create legislation regarding issues that would otherwise be in State control. The Supreme Court ruled that the Driver’s Privacy Protection Act did not violate the Constitution. States are allowed to pass more restrictive privacy protection laws, as long as they meet the minimum level of protection outlined in the Driver’s Privacy Protection Act.

What Information is Protected?

The Driver’s Privacy Protection Act protects the use of personally identifiable information maintained in DMV records. Such information may include:

- Legal name, physical address, and phone number
- Social Security number and Driver Identification number
- Photograph and finger prints
- Height, weight, gender, age
- Any medical or physical disabilities

The Act does not protect information regarding traffic violations, accidents or license status.

Consent of the individual is required prior to the use and disclosure of their information unless they meet one of the following permissible uses:

- Required for legitimate agency functions
- Required for insurance purposes
- Required to verify the accuracy of information in a transaction initiated by the customer
- Related to Motor vehicle safety including, theft, emissions and notifying customers regarding product recalls
- Related to a civil, criminal or other legal proceeding
- Motor vehicle market research and surveys
- Required for research activities and statistical reports as long as the PI is not disclosed or used to contact individuals
- Required to provide notice of towed or impounded vehicles
- Used by licensed investigators and security professionals
- Used by private toll transportation facilities
- For any requestor when they can provide express written consent of the individual

The Driver’s Privacy Protection Act also requires all Motor Vehicle offices to ensure that all resellers of data comply with the DPPA and that no reseller may use or disclose the information for anything other than the outline allowable purposes.

**Enforcement of the DPPA**

The Driver's Privacy Protection Act created a minimum base of protection, which is the responsibility of each state to implement and Enforce. All states were required to enact adequate protections as outlined by the DPPA as of September 1997. It is the responsibility of State attorneys general to enforce compliance. Any individuals found to be in known violation of the Driver’s Privacy Protection Act may face civil actions and fines of up to $5,000 for each day of noncompliance.

**Summary**

The Driver’s Privacy Protection Act (DPPA) is a federal law that regulates agencies controlled on the state level.

**CIPP Candidate Preparation**

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with several topics found in this post including:

- Federal vs. state authority (V.A.)
CIPP Applied – Consumer Protection Laws: States Trump Federal

One of the topics continuously covered in the Certified Information Privacy Professional surrounds the Federal Trade Commission and consumer protections for unfair or deceptive trade practices with respect to privacy. Examples of companies changing their privacy policy without notice, not complying with the posted policy, or generally sharing information in less than best practice form results in hefty fines and additional compliance costs and paperwork for the offender. The FTC and State Attorneys General bring these suits against the company for violation of Federal laws/rules/regulations.

Of interest recently was Maine's cigarette labeling law. It is generally understood, and well documented in the CIPP references, that federal regulations define a baseline. If a state law exists after passage of a federal act, the state law must either be struck from books, or rewritten to comply with the new legislation. However, if the state wants to define more stringent regulations (think California and car emissions), that is their prerogative under State's Rights. Maine did just that protecting their state consumers with additional cigarette warning labels, and the cigarette manufacturers brought suit. The Supreme Court upheld Maine's consumer protection law resulting in an additional win for courageous states.

CIPP Candidate Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with several topics found in this post including:

- Federal vs. state authority (V.A.)
Successfully Responding to Data Breaches

A recent Forester Research study revealed that 25% of IT security decision makers and influencers reported at least one data breach over the past 12 months. This shows just how much of a reality data breaches are. Unfortunately, it is all too common for organizations to rest easy, thinking that it’s implemented all the appropriate security features to prevent a data breach. The statistics show that planning for the inevitable and knowing that each and every breach is different is absolutely crucial for data protection. This article takes a closer look at the issues involved in responding to data breaches of all kinds.

Perception is Reality

When data breaches occur, it’s important to remember that perception is reality. Successful breach responses take into consideration the framework within which organizations operate. There are various types of breaches, and differing levels of harm perceived with each of them. Successful organizations are able to respond proportionately to the level of harm involved.

Typically, once a data breach is discovered, organizations focus on pre-response activity. This involves understanding what happened, and how it happened. Pre-response activity involves legal and forensic teams where necessary. While such activity may take hours or even months, it’s crucial to note that it must culminate in a Decision to Notify.

Current US breach notification laws require organizations to notify consumers of a data breach within 5 to 60 days. Within this time frame, organizations must begin mailing notifications to affected consumers. This notification normally triggers phone calls, so the organization must also set up a call center to receive the calls and respond to the questions and inquiries the customers are certain to have.

According to an AllClear ID report on data breaches, almost 20% of notice letter recipients will call the organization. These calls usually last anywhere from 5 to 20 minutes, so organizations must be prepared to serve customers with multiple channels of communication. Even if an 800-phone number is included in the notification letter, some customers will also choose to use email or social media channels. Ensure that physical and digital locations are aware of what to expect and where to relay information.
Reducing the Cost of a Breach

Responding with concern to customer inquiries can save organizations millions in third-party legal fees, liabilities and lost business. In fact, lost business often ends up being the greatest cost of a data breach. According to a 2010 US Cost of a Data Breach study conducted by the Ponemon Institute, the typical breach costs $214 per record in both fixed costs and lost business.

Another recent Ponemon study showed a 21% average diminished value for brands after a breach, and an average of one year to restore an organization’s reputation. A poorly executed breach response on top of an already worrisome customer event only serves to increase damages.

While there are a number of remediation approaches, one of the most common is to enroll customers in an identity theft protection product, which includes both credit monitoring and fraud assistance. It’s also important to limit third-party liability exposure and act in the best interests of the affected individuals, given that regulations are becoming increasingly stringent in terms of consumer privacy protection.

Types of Breaches

Being aware of the different types of identity theft can help an organization assess the risk of harm involved in a data breach and respond appropriately. There are four main categories of identity theft, each with a different level of harm.

- Financial identity theft
- Employment identity theft
- Medical identity theft
- Criminal identity theft

Financial Identity Theft

This is the most common type of identity theft that arises from a data breach. Experts have identified two different risk factors:

Existing account takeovers – These involve fraudulent transactions with compromised account numbers.

New account fraud – This involves compromised personally identifiable information (PII), which is used to obtain new credit, utility and/or service accounts. Since all that is needed to apply for
and obtain a new account is a Social Security number and date of birth, this represents a particularly high risk.

**Employment Identity Theft**

This form of identity theft is increasing, in part because many organizations maintain a vast amount of sensitive information about their employees, particularly their Social Security numbers (SSNs). As mentioned earlier, SSNs are often all that is necessary to open a new credit account. Child identity theft also presents a large risk, as it can often go undiscovered for many years, until the child turns 18 and starts to create his/her own financial identity. Although employment identity theft isn’t the most common type of theft that results from a data breach, it represents one of the most difficult to restore, given the long-term nature of the fraud and its delayed discovery.

**Medical Identity Theft**

Medical identity theft is closely related to traditional financial identity theft. This happens when someone illegally obtains personal medical or health insurance information and uses it to get medical treatment, prescription drugs or other health care services. This form of identity theft is difficult to prevent, as there is no central repository for health care data to function as a clearinghouse (unlike credit bureaus created for financial data).

Medical identity theft frequently comes with financial consequences, since it results in unpaid bills from hospitals and doctors, or unpaid claims from health insurance companies. This identity theft will inevitably create problems for an individual’s medical and health insurance records, which will have a real and lasting impact on the victim’s health care treatment.

**Criminal Identity Theft**

Criminal identity theft is the least common of the four types of identity theft. However, it is the most difficult to restore, due to the nature of the third parties needed to prove innocence. Criminal identity theft happens when a consumer is held liable for criminal activities he/she did not commit. This type of identity theft is often discovered when a victim is pulled over for a traffic violation and subsequently arrested due to an outstanding warrant. This might have happened because a criminal was arrested and presented a stolen or lost driver’s license, passport or other form of identification. Often, companies that collect or maintain physical or digital copies of personal identification are exposed to this type of data breach.
Summary

Organizations that suffer a data breach must respond appropriately, or they will risk increased losses, both in financial terms and diminished brand perception. Each type of data breach has an associated level of harm, so it’s important that decision makers within the organization know how to evaluate and respond to the various breaches. The article looks at the four main categories of identity theft which may arise when a breach occurs: 1) financial identity theft; 2) employment identity theft; 3) medical identity theft; and 4) criminal identity theft.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Data breach notification laws (V.E.)
CIPP Applied – NASA under Attack

NASA’s security history in recent months has suffered major attacks. For instance, In March 2011, someone exposed algorithms used to command and control the International Space Station. Then, in March 2012, the personally identifiable information (PII) of 2,300 employees and students was leaked. In yet another embarrassing incident, some sensitive data was breached from NASA’s Constellation and Orion programs. Finally, on October 31, 2012, PII on an unspecified, yet substantial, number of NASA employees and contractors was leaked.

Between April 2009 and April 2011, NASA reported the loss or theft of 48 of its mobile computing devices, according to the NASA Watch Blog, a loud critic of the agency’s data protection practices.

Unencrypted Employee Data

In this most recent data breach, NASA sent a warning to all employees and contractors after a thief stole a NASA laptop and other documents from an agency employee’s locked car. Richard J. Keegan, Jr., associate deputy administrator of NASA wrote:

“On October 31, 2012, a NASA laptop and official NASA documents issued to a headquarters employee were stolen from the employee’s locked vehicle. The laptop contained records of sensitive personally identifiable information (PII) for a large number of NASA employees, contractors and others.”

This wasn’t the only piece of bad news. It turned out that the data on the laptop was not protected by encryption technology. “Although the laptop was password protected, it did not have whole disk encryption software, which means the information on the laptop could be accessible to unauthorized individuals,” Keegan’s notice read.

Currently, NASA has not determined the full extent of the breach. It's assumed that the agency is still attempting to reconstruct and study all the data that had been stored on the stolen laptop. “Because of the amount of information that must be reviewed and validated electronically and manually, it may take up to 60 days for all individuals impacted by this breach to be identified and contacted,” Keegan said.

Remediation Efforts

Being just the latest example of a number of data breaches, all involving the theft of unencrypted NASA laptops, the agency has finally seen the need to address the situation. NASA’s Chief Information Officer, Linda Cureton, has since ordered that all agency laptops be encrypted within a month. The agency’s CIOs must complete whole disk encryption of the maximum possible number of laptops by November 21, 2012. The effort is expected to be completed by December 21, 2012, after which no unencrypted laptop, regardless of whether it
contains PII, will be allowed to leave its facilities. Furthermore, employees have been banned from storing sensitive data on mobile phones, tablets and other portable devices.

NASA is also taking other standard breach precautions, which include contracting a data breach specialist – ID Experts – to notify those whose PII was compromised. The agency has offered free credit and identity monitoring, recovery services in cases of identity compromise, an insurance reimbursement policy, educational materials, access to fraud resolution representatives and a call center and website.

The agency has recommended that those affected should be wary of suspicious phone calls, emails and other communications from individuals claiming to be from NASA, or other official sources that ask for personal information or verification of it.

Terry Greer-King, the UK managing director for security firm Check Point, commented that the fact that this latest breach comes so soon after a similar incident in March proves that enforcing good data security is an ongoing, rigorous process. “By its own admission, only 1% of NASA laptops and portable devices were encrypted as of February 2012, compared with a US government-wide encryption rate of 54%,” Greer-King said.

“This shows that there is still a long way to go before the data held on government and corporate laptops is truly secure,” he went on to observe.

Summary

This article takes a look at NASA data breaches since 2011, most of which have involved stolen laptops which contained sensitive or personally identifiable information (PII) that were not protected by encryption technology. The most recent data breach was announced on October 31, 2012, and resulted in agency-wide changes to the handling and protection of PII. NASA’s Chief Information Officer has since ordered that all agency laptops be encrypted by December 21, 2012.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) and the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Data breach notification (V.E.)
Anti-Bullying Legislation in the United States: Children & Cyberbullying

Both state and local lawmakers have taken action to protect children and prevent bullying. Many states have enacted laws in state education codes, among other places as well as created model policies, which provide guidance to school districts. Bullying, cyberbullying, and other such behaviors may be addressed in a single law, or through multiple pieces of legislation. In certain cases, bullying appears in the section of a state criminal code that applies to juveniles.

What does bullying look like?

In this context, the US government defines bullying as “unwanted, aggressive behavior among school aged children that involves a real or perceived power imbalance. The behavior is repeated, or has the potential to be repeated, over time.” Those who are involved in bullying, whether directly or indirectly, may have serious, long-lasting problems. Bullying can include actions such as making threats, spreading rumors, attacking someone physically or verbally, and excluding someone from a group on purpose.

There are three recognized types of bullying:

1. Verbal bullying
2. Social bullying (also referred to as relational bullying, which damages an individual’s reputation or relationships)
3. Physical bullying (doing harm to a person’s body or possessions)

According to the 2011 Youth Risk Behavior Surveillance System, 20 percent of students nationwide in grades 9 to 12 have experienced bullying. The 2008-2009 School Crime Supplement also indicated that nationwide, 28 percent of students in grades 6 to twelve have experienced bullying.

Cyberbullying

Cyberbullying is bullying that occurs via electronic technology. Such technology includes devices such as mobile phones, computers and tablets, as well as communications tools like social media sites, text messages, chat and websites.

Children who are victims of cyberbullying are often bullied in person. Children who are being cyberbullied often have a more difficult time getting away from the behavior. This is because cyberbullying can take place 24/7, affecting a child even when he/she is alone. Such messages and images can be posted anonymously and distributed quickly to a large audience, making it difficult or even impossible to trace the source. Furthermore, deleting inappropriate or harassing messages, texts and pictures is extremely difficult after they have been posted or sent out.
According to the 2008-2009 School Crime Supplement, 6 percent of students in grades 6 to 12 have experienced cyberbullying. The 2011 Youth Risk Behavior Surveillance Survey reported that 16 percent of high school students were electronically bullied in 2010.

**State Legislation Only**

To date, there is no federal law that specifically applies to bullying. In certain cases, when bullying is based on race, color, national origin, sex, disability or religion, bullying overlaps with harassment and schools are legally obligated to address it. Although the No Child Left Behind Act of 2001 provides federal support to promote school safety, it does not specifically address bullying and harassment in schools.

Since 1999, 49 states have passed school anti-bullying legislation. The only state lacking such legislation is Montana.

In 1999, Georgia was the first state to enact a school anti-bullying legislation, which was strengthened in 2010 by the passage of Senate Bill 205. This bill included a provision allowing for those accused of bullying another student to be reassigned to a different school, in order to separate the offender from the victim.

In September 2011, New Jersey began enforcing what is considered the most stringent anti-bullying law in the country. The NJ Anti-Bullying Bill of Rights Act requires each school to report each case of bullying to the state. The state will then grade each school based on bullying standards, policies and incidents.

**What does an anti-bullying policy look like?**

Watchdog organizations and anti-bullying advocates have identified eleven important components of effective anti-bullying policies. These components are listed below:

1. Purpose statement
2. Statement of scope
3. Specification of prohibited conduct
4. Enumeration of specific characteristics
5. Development and implementation of local educational agency (LEA) policies
6. Components of LEA policies:
   a. Definitions
   b. Report bullying
   c. Investigating and responding to bullying
d. Written records  
e. Sanctions  
f. Referrals  

7. Review of local policies  
8. Communication plan  
9. Training and preventive education  
10. Transparency and monitoring  
11. Statement of rights to other legal recourse

Summary

Unfortunately, bullying and cyberbullying is a serious issue that affects a significant number of school-aged children. To date, no federal anti-bullying law exists, though 49 states have enacted anti-bullying laws protecting children from bullying.

CIPP Exam Preparation

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Anti-bullying laws (V.F.)
Anti-Bullying Legislation in the United States: Workplace Bullying

Anti-bullying legislation has been promoted by workplace advocates for many years. So far, twenty-three states have introduced workplace bullying legislation known as The Healthy Workplace Bill, however no laws have been enacted. Eight states were active as of early 2013 with eleven current bills.

What does workplace bullying look like?

According to the Healthy Workplace Campaign, workplace bullying is a “repeated, health-harming mistreatment of one or more persons (the targets) by one or more perpetrators.” Workplace bullying can take any of the following forms:

- Verbal abuse
- Offensive conduct/behaviors (including nonverbal actions) which are threatening, humiliating or intimidating
- Work interferences (i.e. sabotage), which prevents work from being done

Recent statistics show that workplace bullying affects the lives of 37 percent of adult Americans. In its more severe forms, it is related to several stress-related health complications (e.g. hypertension, auto-immune disorders, depression, anxiety and PTSD). Often, the individual’s immediate job and career are disrupted.

Other statistics on workplace bullying include:

- 49 percent of adult Americans have been bullied, or witnessed it in the workplace
- 80 of bullying is legal
- 72 percent of bullies outrank their targets in the workplace (i.e. bullies are their targets’ bosses or supervisors)

This is a serious concern for employers, as it is often the least skilled employees who attack better workers, because of the perceived threat they imagine. When the perpetrator has the power to deprive his/her target of a livelihood and the economic and health security the job represents, bullying is an abuse of authority.

No Federal Framework

Currently, there is no federal law expressly prohibiting bullying in the workplace, or otherwise. Although efforts at prohibiting bullying in the education sector have begun at the state level, there has been no serious effort to enact legislation covering bullying in the workplace. This
leaves workplace bullying victims to work through a patchwork of other federal and state laws that may encompass the bullying behavior at issue, though they may not necessarily be directed at bullying.

Victims may seek some protection through state common law torts, such as intentional infliction of emotional distress, or battery. For instance, if the bullying behavior included offensive, unwelcome touching, there might be grounds for civil battery.

Federal employment laws may also offer some protection for bullying victims, but that protection is dependent upon the bully’s motive, which must be based upon the victim’s protected status. For instance, if the bully is motivated by the victim’s race, such that he has targeted individuals of Asian descent for bullying, but not whites, that bully behavior could constitute a racially hostile work environment. However, if the bully is motivated by a personal dislike for the victim unencumbered by a racial or gender bias, the federal employment laws would offer no such protection.

Healthy Workplace Bill

Since 2001, the Healthy Workplace Campaign has been working towards anti-bullying laws on a state-by-state basis. What is now known as the Healthy Workplace Bill (HWB) was drafted by David Yamada, a law professor at Suffolk University. The HWB has been introduced in twenty-three states, in over sixty versions, and has been sponsored by more than three hundred legislators.

In brief, here are some important aspects of the HWB for employers:

- Defines an “abusive work environment” – a high standard for misconduct
- Requires proof of health harm by licensed health or mental health professionals
- Protects conscientious employers from vicarious liability risk when internal correction and prevention mechanisms are in effect
- Gives employers the reason to terminate or sanction offenders
- Requires plaintiffs to use private attorneys
- Fills the gaps in current state and federal civil rights protections

Some important aspects of the HWB for employees:

- Provides an avenue for legal redress for health-harming cruelty at work
- Allows employees to sue the bully as an individual
- Holds the employer accountable
- Seeks restoration of lost wages and benefits
- Compels employers to prevent and correct future instances
However, the HWB does not:

- Involve state agencies to enforce any provisions of the law
- Incur costs for adopting states
- Require plaintiffs to be members of protected status groups (i.e. it is “status-blind”)
- Use the term “workplace bullying”

**Outside the US**

It’s important to note that the US is the last western democracy without a law forbidding workplace bullying. Since 1994, Scandinavian nations have enacted explicit anti-bullying laws. Many of the EU nations have significant legal employee protections compelling employers to prevent or correct bullying.

Britain – which coined the term “workplace bullying,” has broad anti-harassment laws which also cover bullying, while Ireland’s stringent health and safety code addresses bullying.

Canada’s first provincial law on workplace bullying was enacted in 2004, the second in 2007, and another in 2010. The issue is also covered in the occupational health code for federal employees in 2008.

**Summary**

Workplace bullying is an issue which has directly or indirectly affected almost half adult Americans. This article takes a look at what constitutes “workplace bullying,” and the state legislation that has been adopted to deal with the problem. The article introduces the Healthy Workplace Campaign and the Healthy Workplace Bill.

**CIPP Exam Preparation**

In preparation for the Certified Information Privacy Professional/United States (CIPP/US) exam, a privacy professional should be comfortable with topics related to this post, including:

- Anti-bullying laws (V.F.)
## State Security Laws

<table>
<thead>
<tr>
<th>Who is covered?</th>
<th>n/a</th>
</tr>
</thead>
</table>
| What is covered? | - “Personal information” – any data elements that trigger breach notification laws. May/may not include name.  
- Processing of SSNs. |
| What is required or prohibited? | - Reasonable security  
- Controls similar to GLBA  
- Appropriate disposal of media and paper records |
| Who enforces the law? | - State Attorneys General  
- Private rights of action |
| What happens if there is no compliance? | - Enforcement actions  
- Private lawsuits  
- Statutory damages |
| Why does the law exist? | - To improve corporate and government commitment to information security.  
- To ensure that companies are responsible for protecting sensitive information of state citizens. |

## California SB 1386 – Security Breach Notification Law

<table>
<thead>
<tr>
<th>Who is covered?</th>
<th>Entities that do business in California (CA).</th>
</tr>
</thead>
</table>
| What is covered? | - Computerized personal information (PI) of CA residents.  
- PI = name plus SSN, drivers’ license, financial account numbers/access codes, medical information and health insurance information. |
| What is required or prohibited? | If unencrypted PI is accessed inappropriately, prompt notice must be provided to affected individuals. |
| Who enforces the law? | - CA Attorney General – aggressively enforced  
- Private right of action – as do most CA laws |
| What happens if there is no compliance? | Liability for monetary damages ($2500/violation). |
| Why does the law exist? | Concern that security breaches would cause identity theft. |
California SB 1: California Financial Privacy Law

<table>
<thead>
<tr>
<th>Who is covered?</th>
<th>Domestic FIs</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is covered?</td>
<td>Non-public personal financial information</td>
</tr>
<tr>
<td>What is required or prohibited?</td>
<td></td>
</tr>
<tr>
<td>• FIs must offer opt-out if personal information is being shared with affiliates or joint marketing partners.</td>
<td></td>
</tr>
<tr>
<td>• FIs can share personal information with non-affiliates only if opt-in consent is provided.</td>
<td></td>
</tr>
<tr>
<td>Who enforces the law?</td>
<td></td>
</tr>
<tr>
<td>• CA state banking regulators</td>
<td></td>
</tr>
<tr>
<td>• CA Attorney General</td>
<td></td>
</tr>
<tr>
<td>• Private rights of action</td>
<td></td>
</tr>
<tr>
<td>What happens if there is no compliance?</td>
<td></td>
</tr>
<tr>
<td>• Enforcement actions</td>
<td></td>
</tr>
<tr>
<td>• Private lawsuits</td>
<td></td>
</tr>
<tr>
<td>Why does the law exist?</td>
<td>To extend requirements of the GLBA.</td>
</tr>
</tbody>
</table>

Driver’s Privacy Protection Act (DPPA)

- Protects the use of PII maintained in DMV records.
- Does not protect information regarding traffic violations, accidents or license status.
- All states required to enact adequate protections; it is state responsibility to implement and enforce minimum protections outlined by DPPA.

Data Breaches

- Organizations must notify consumers of data breaches within 5 to 60 days.
- Types of breaches:
  - Financial ID theft – existing account takeovers; new account fraud
  - Employment ID theft – SSNs at risk
  - Medical ID theft – unauthorized access to personal medical or health insurance information
  - Criminal ID theft – least common, most difficult to restore
Anti-Bullying Legislation

- School bullying: verbal, social, physical
- Cyberbullying = bullying via electronic technology
- 49 states have school anti-bullying legislation
- Workplace bullying: verbal abuse, offensive conduct/behaviors, work interferences
- No federal laws that specifically apply to bullying (school or workplace)
- Draft of Healthy Workplace Bill 2001 (HWB)
## Definitions

| Access | This is the ability to view personal information held by an organization. Access may also include the ability to update or correct the information.  
In the US, access is required by law for substantive decision-making. |
| --- | --- |
| Choice | This is the ability to specify whether personal information will/will not be collected. It also relates to how the information will be used.  
Under US law, choice is often required for marketing communications. |
| Civil Litigation | When one person sues another in order to correct contract disputes, on the basis of common law tort claims or to enforce a law. |
| Classification | US laws focus on types of data. Classification is based on sensitivity of data. |
| Commercial Electronic Mail Messages | Email messages with a primary purpose of advertising a product/service. |
| Consumer | An individual (natural person) who is acting in a personal (e.g. family or household) capacity. |
| **Consumer Report** | Any information relating to:  
| | • credit worthiness  
| | • credit standing  
| | • credit capacity  
| | • character  
| | • general reputation  
| | • personal characteristics  
| | • mode of living  
| | Such information is used to establish eligibility for credit, insurance, employment or some other business purpose. |
| **Consumer Reporting Agency (CRA)** | Any organization responsible for assembling or evaluating consumer information to provide consumer reports to third parties. |
| **Criminal Litigation** | When the executive branch of government sues a person for violation of a criminal law. |
| **Deceptive Trade Practice** | Commercial actions that involve false or misleading claims. See also “Unfair Trade Practices.” |
| **Financial Institution (FI)** | Any entity significantly engaged in financial activities. |
| **Investigative Consumer Report** | Information about an individual gathered from interviews with third parties (e.g. neighbors, friends). Regulated by the FCRA (Fair Credit Reporting Act). |
| **Jurisdiction** | Refers to the authority of a court or government agency to handle a particular case. Courts require both subject matter jurisdiction and personal jurisdiction.  
| | For instance, the FTC (Federal Trade Commission) has the jurisdiction to handle consumer protection matters in all areas except banking. |
| **Negligence** | Negligence refers to the breach of a duty that results in harm and damages to an individual. Organizations found to be negligent may be liable for damages, which may be economic or non-economic. |
| **Notice** | This refers to a description of an organization’s information management practices. Notices are developed for the purposes of consumer education as well as corporate accountability. |
| **Pen Register** | Indicates the numbers called from a particular instrument.  
| | See also: trap-and-trace device. |
| **Person** | Any entity with legal rights. This may include an individual (considered a “natural person”) as well as a corporation, trust or government agency (“legal person”). |
| **Preemption** | This is a conflict of law doctrine. Preemption exists when a superior government’s laws supersede those of an inferior government. For instance, if Congress decides to pass a law, state governments cannot regulate in that area. The Federal FCRA (Fair Credit Reporting Act) preempts any state laws regarding credit reports. |
| **Self-Regulation** | Members of industry organizations with self-regulatory codes are bound to following these codes. Disregarding self-regulatory codes may result in legal liability. |
| Industry organizations include: |
| • BBB – Better Business Bureau Online |
| • TRUSTe |
| • DMA – Direct Marketing Association privacy promise |
| • CARU – Children’s Advertising Review Unit |
| **Trap-and-Trace Device** | A trap-and-trace device identifies the source of incoming calls. |
| See also: pen register. |
| **Unfair Trade Practices** | Commercial conduct that can cause injury without offsetting benefits to the consumer. Consumers cannot reasonably avoid these practices. See also “Deceptive Trade Practices.” |
Appendices

CIPP Prep Guide
CIPP/US Concentration

Appendix A – The CIPP/US CBK Outline