

Taylor McEldowney

College: Boston College (Carroll School of Management)

Major: Finance and Marketing (Minor in Environmental Studies)

Companies hosting cloud computing services monitor and control communication and data stored between the user and the host company. This creates numerous privacy problems, as there is little end-user knowledge of what the hosts do with the data and who can access it. As a result many data privacy laws concerning businesses, individuals and the government, have been enacted at all levels to make sure that data is protected and not corrupted.

Data privacy is very important for businesses because they control a great deal of important data about their customers, such as financial information and addresses. The International Organization for Standards provides a “model for establishing, implementing, operating, and monitoring an Information Security Management System” (Gallagher 281). This helps companies more efficiently handle data privacy. This type of model can be used to comply with the various data privacy laws that businesses face. For example The Fair Credit Reporting Act is a federal law that regulates the collection, distribution, and use of consumer information that will be used for credit evaluation. This allows consumers to be aware of what data others will see. Also the Right to Financial Privacy Act, another federal law, ensures data security for customers of financial institutions so they feel safe when disclosing their personal information. Although according to U.S. v Miller, financial records are the property of financial institutions not the customers, these institutions are only allowed to disclose these records if there is a warrant or the customer agrees (12 U.S.C. 3414). Finally there are laws that deal with special issues such as the Health Insurance Portability and Accountability Act, which regulates health data, the Graham-Leach-Bliley Act, which regulates financial data and the Children’s Online Privacy Protection Act, which regulates data collection on minors (Gallagher 281). All companies that hold data must follow regulations about disclosing personal information to make people feel safe and protected when releasing their personal information.

Individuals also possess data security from laws and regulations. The Data Protection Directive of the European Union grants every member of the EU the right to access their data and the right to object to processing of this data. It also ensures that any data is processed fairly and lawfully (Directive 95/46/EC). This provides all individuals in the EU with data security. There are also data protection laws in place for individuals in New England. In 2010, Massachusetts passed Standards for the Protection of Personal Information of Residents of the Commonwealth, which requires all companies that possess information about Massachusetts's residents to have an information security program and a security system (201 CMR 17.00). While Massachusetts's law is the most radical, Rhode Island also has a proactive data privacy law. Maine, Vermont, and New Hampshire only have reactive data laws, which are the most common among states. These require that companies who compromise data of residents of these states must follow certain steps after the breach. Finally individuals also possess special protection from other acts such as the Driver's Privacy Protection Act of 1994, which regulates information shared by DMV or automotive companies and the Family Educational Rights and Privacy Act, which provides rights to school records. Because individuals release much of their personal information to others, they require certain protections to make sure this data is always protected.

Finally the government also has data privacy regulations. The Federal Information Security Management Act of 2002 requires that all federal agencies implement programs that address information security. In addition, these federal agencies must protect all information from unauthorized access, disclosure, modification and destruction. The Computer Fraud and Abuse Act deals with data privacy issues related to the use of federal computers. This act makes it illegal for anyone to knowingly or intentionally access a computer or affect its operation without authorization (18 USC 1030). Because the government deals with very important data, they need to have extra measures of protection.

Although data privacy is important for all three of these groups, it is most relevant to businesses. However, there are still many instances in which customers' data privacy is breached. This needs to be solved. Although there are many laws that businesses are forced to comply with, compliance does not always equal security. For example, Heartland Payment

Systems, a credit card processing company, complied with all of its data security regulations, however, they still experienced a data security breach. In this breach, over 100 million people's credit cards information was compromised. This shows that for a business to truly be secure it needs to have a complete organizational commitment to data protection. A firm needs to not just comply, but take all measures to ensure that the firm is secure for all of its stakeholders. Most employees do not know what kind of data their company collects and how it should be properly protected. Furthermore only about 24% of companies keep an inventory of the data they collect (Gallagher 282). This should be changed so that all company members are aware of their collected data and its uses to truly protect all their stakeholders. Because large companies hold the most important data, they need to implement company wide data security systems and data privacy values to protect all individuals.

Data privacy has become a very prominent issue with the evolution of technology. As a result many different legal and regulatory frameworks have been enacted to ensure data security regarding businesses, individuals, and governments. All three have certain requirements they must follow and protections they are entitled to receive. However, it takes more than just compliance with these regulations to be truly secure. Data privacy needs to be incorporated into all areas to ensure the protection and security of all people and their personal information.

Works Cited

Directive 95/46/EC. European Union. Data Protection Directive of the EU. European Parliament. Euro-Lex, 24 Oct. 1995. Web. 20 Mar. 2011. <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT>>

Gallaugh, John. Information Systems. Nyack, NY: Flat World Knowledge, 2010. Print.

18 USC 1030. Computer Fraud and Abuse Act. Legal Information Institute of Cornell University. 1986. Web. 20 Mar. 2011. <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html>

18 U.S.C. 2721-2725. Driver's Privacy Protection Act of 1994. Legal Information Institute of Cornell University. 1994. Web. 20 Mar. 2011. <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002721----000-.html>

20 U.S.C. § 1232g; 34 CFR Part 99. Family Educational Rights and Privacy Act. U.S. Department of Education. 1974. Web. 20 Mar. 2011. <<http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>>

44 U.S.C. § 3541. Federal Information Security Management Act of 2002. U.S. Department of Homeland Security. 17 Dec. 2002. Web. 20 Mar. 2011. <[http://www.marcorsyscom.usmc.mil/sites/pmia%20documents/documents/Federal%20Information%20Security%20Management%20Act%20\(FISMA\).htm](http://www.marcorsyscom.usmc.mil/sites/pmia%20documents/documents/Federal%20Information%20Security%20Management%20Act%20(FISMA).htm)>

12 U.S.C. 3414. Right to Financial Privacy Act of 1978. Federal Deposits Insurance Corporation. 1978. Web. 20 Mar. 2011. <<http://www.fdic.gov/regulations/laws/rules/6500-2550.html>>

15 U.S.C. § 1681. Federal Trade Commission. Fair Credit Reporting Act. Federal Trade Commission. 29 June 1968. Web. 20 Mar. 2011. <http://www.ftc.gov/os/statutes/fcradoc.pdf>

201 CMR 17.00. Massachusetts. Standards for the Protection of Personal Information of Residents of the Commonwealth. Massachusetts Government, 2010. Web. 20 Mar. 2011. <<http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>>