AN ENTREPRENEUR'S GUIDE TO DATA PRIVACY LAW IN THE UNITED STATES AND EUROPEAN UNION[I]

by

Brian P. Kalis[*]

1 INTRODUCTION

Data privacy is the international human rights issue of the new Millennium.[1] The rise in the use of the Internet and the globalization of markets has eliminated traditional barriers that separate people and keep private most of their lives.[2] The Internet has made it easy to access and compile a wealth of information about a person that was once difficult and time-consuming to obtain.[3] The United States (U.S.) and European Union (EU)[4] "have basic philosophical and cultural differences in the way they view personal privacy rights."[5] The philosophical and cultural differences are evident in the way the two nations approach data privacy regulation. The EU uses proactive national legislation to protect data privacy in the public and private sectors. The U.S., in contrast, uses a combination of legislation, regulation, and self-regulation to protect data privacy. U.S. regulation of data privacy protection is typically implemented in response to data privacy abuses. These different approaches to data privacy regulation had to be reconciled when the EU passed the Data Privacy Directive on October 24, 1995,[6] which prohibits data transfers to non-EU nations who do not have "adequate protection."[7] The U.S. does not have "adequate" protection according to the Directive. As a result, the U.S. Department of Commerce (Department of Commerce) negotiated the Safe Harbor Agreement (Safe Harbor) with the EU so U.S. businesses could self-regulate to meet the Directive's "adequacy" standard.[8] Continued extraterritorial application of data privacy laws in the global marketplace may create conflicts between countries that will bring data privacy rights to the forefront of the international human rights debate.

Information technologies and the Internet have made it easy for large and small businesses to collect, process, store, and disseminate personally identifiable information[9] quickly and inexpensively.[10] Businesses regularly exchange or sell personally identifiable information to create complex consumer profiles that are used to target products and services to consumers.[11] Consumer profiling and targeting has become increasingly important in the competitive environment of a global marketplace. As a result, the collection, processing, storage, and transfer of personally identifiable information in the public and private sectors has become an increasing concern of private citizens, consumer groups, and national governments as they seek less intrusion upon their personal lives.[12] The increased concern about the use of personal information has led to the adoption of data privacy laws in the U.S. and EU that affect all sizes of businesses across all sectors.

The escalating concern about how personal information is used and the adoption of data privacy laws impact entrepreneurs in the U.S. and the EU. For example, entrepreneurs may have to implement data protection measures into their business models to meet the increasing privacy demands of their consumers. Furthermore, a majority of the data privacy laws do not include exemptions for small and medium size enterprises (SMEs),[13] so entrepreneurs will have to implement data protection measures to adhere to government mandates. The consumer and legal expectations for data protection measures are the same for SMEs and large enterprises. However, SMEs should not only be concerned about consumer demands and federal mandates for data protection. SMEs should also be concerned about data protection because computer security breaches have been increasing in recent years.[14] A 2002 survey by the FBI found that "90% of respondents detected computer security breaches in the past year."[15] Computer security weaknesses may allow an attacker to access a SMEs' confidential and personally identifiable information that may be used and abused by an attacker. Access to a SMEs' proprietary information could threaten the businesses going concern if unauthorized people access the information. As a result, all SMEs should develop and implement organizational and technical data protection measures to ensure the protection of all organizational data, including personally identifiable information. Proactive data protection is smart business; will ensure that a SMEs' information is protected; and make compliance with current and nascent data privacy laws easier.

This article provides an overview of data privacy laws in the U.S. and the EU of particular concern to U.S. entrepreneurs. This article will also advocate that an entrepreneur in the U.S. should develop and implement basic data protection measures to protect their data, including any personally identifiable information they may collect, process, store, and disseminate. Part II of this article provides an overview of entrepreneurship in the U.S. and EU. It is important for an entrepreneur to understand different cultural approaches toward entrepreneurship in the countries in which they may engage in business. This is increasingly important in a global economy. Part III of this article will provide an overview of the history of data privacy law in the EU. Part IV of this article provides an overview of the history of data privacy law in the U.S. and advocates that an entrepreneur in the U.S. should develop and implement basic data protection measures to protect their data regardless of a lack of a broad based national data privacy law. Parts III and IV include commentary on the implications of data privacy laws on entrepreneurial ventures. The information in this article is important for entrepreneurs who may pursue

regional and international business opportunities in countries with proactive data privacy laws. This article is especially important for entrepreneurs interested in pursuing business opportunities that result as the EU moves towards enlargement in the coming year with the inclusion of ten Eastern European nations.[16] The ten Eastern European nations have been adopting the entire body of EU law know as the *acquis acommunitaire* (*acuqis*) to meet EU membership criteria.[17] The Directive is a part of the *acquis* that the ten Eastern European nations have been implementing into national law over the past few years. As a result, an entrepreneur who pursues business opportunities in the ten Eastern European nations must comply with the Directive or potentially face blocked data transfers, fines, or criminal penalties.

2 ENTREPRENEURSHIP IN THE U.S. AND EUROPE

As a preliminary matter, entrepreneurship differs in the U.S. and EU. This section provides a brief overview of entrepreneurship in general and some of the cultural and legal factors that influence entrepreneurship. Entrepreneurship is "the process of organizing, managing, and assuming the risks of a business"[18] for profit. Entrepreneurship is important because entrepreneurs help stimulate national and regional economic growth "through their leadership, management, innovation, research and development effectiveness, job creation, competitiveness, productivity, and formation of new industry."[19] "Entrepreneurialism also tends to challenge barriers of ideology, social caste, and tradition and engender new demands for political freedoms."[20] The "cultural climate in which a would-be entrepreneur lives and breathes"[21] influences their willingness and desire to become an entrepreneur. It is important for an entrepreneur who may captivate on international business opportunities to understand the entrepreneurial context—individual, governmental, and societal factors that affect entrepreneurship— in the countries in which it intends to do business. This section will provide a brief overview of the entrepreneurial context in the U.S. and EU.

2.1 THE ENTREPRENEURIAL CONTEXT IN THE U.S.

The U.S. is more entrepreneurial than the EU.[22] This is evident because the U.S. has more people than the EU that: 1) prefer self-employment to employment;[23] 2) thought of starting a business;[24] 3) started or are taking steps to start a business;[25] and 4) are willing to take the risks associated with starting a business.[26] Citizens of the U.S. and the EU list the lack of financial resources and administrative complexity as the main barriers to starting a business.[27] These barriers must be minimized to help stimulate entrepreneurial activity.

Overall, the culture and legal system of the U.S. encourages and supports entrepreneurial activity. The following is a list of some examples of cultural and legal measures that foster entrepreneurship:

- Legal regime for contracts and contract enforcement;[28]
- Intellectual property laws that allow an entrepreneur to profit from innovation;[29]
- Liberal bankruptcy laws;[30]
- Tax system that supports business activity;[31]
- Government financial support of risky ventures, such as the creation of the Internet, that stimulate entrepreneurial activity;[32]
- Subsidized government loans for small business owners;
- Government agencies that aid small businesses;
- Educational system that "generate research, skilled workers, and managers;"[33]
- Financial markets that finance new businesses;
- "Culture [that] stresses personal improvement, loves novelty and change, excels at technological ingenuity, and celebrates the making of money;"[34]
- Fair and open markets.[35]

2.2 ENTREPRENEURIAL CONTEXT IN THE EUROPEAN UNION

The Member States of the EU are less supportive of entrepreneurial endeavors. It is difficult to generalize about cultural and legal factors in the EU that impact entrepreneurship because the EU is composed of fifteen countries with distinct national cultures and legal systems.[36] "In general, smaller nations tend to be more international in perspective and more resourceful in pursuing their economic opportunities."[37] Larger European nations, such as Germany, France, and Great Britain, are "more resistant to change and less internationally minded"[38] than their smaller counterparts. In general, some of the cultural and legal factors that discourage entrepreneurship in the EU are as follows:

- High taxes;[39]

- Bankruptcy laws that favor creditors;[40]
- Strict labor laws;[41]
- Strong central government control;
- Social programs that favor labor;[42]
- Lack of an entrepreneurial attitude;[43]
- Conservative, risk averse financial system that will not finance new business ventures.[44]

However, the common currency and internal market of the EU may stimulate more entrepreneurial activity in the future as barriers to trade are eliminated and the size of the internal market increases.[45] Moreover, there is an increasing interest in self-employment in younger age groups in Europe that may stimulate entrepreneurial activity within the next decade.[46]

It is apparent from the information in this section that the EU prefers proactive regulation of business to the reactive regulatory model of the U.S. These differing approaches to regulation are also apparent in the way the U.S. and EU have approached the issue of regulating how businesses of all sizes protect personally identifiable information.

3 HISTORY OF DATA PRIVACY LAW IN THE EUROPEAN UNION

The European approach to data privacy law is based on the belief that an individual's personal privacy is a fundamental human right that should be protected by law. This approach began to develop in Europe after World War II (WWII).[47] One of the first occurrences of the notion of a fundamental human right to privacy after WWII is in Article 12 of the United Nations' *Universal Declaration of Human Rights* (Declaration) of 1948.[48] The Declaration recognized the right to the protection of law against interference or attacks related to an individual's "privacy, family, home or correspondence."[49] Article 12 of the Declaration was echoed in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (Human Rights Convention) of 1950.[50] The Human Rights Convention uses wording similar to the International Declaration to declare an individual's right to "respect for his private and family life, his home and his correspondence."[51] Although the Human Rights Convention recognized privacy as a fundamental human right in 1950, the transition of Europe's economy from an industrial economy to an information economy in the 1960s[52] and the increased use and availability of computing technology[53] were the impetus for the creation of data protection laws in Europe.

The first data protection laws emerged in Europe in the 1970s in "response to a privacy movement in the U.S. during the 1960s and 1970s"[54] that was driven by the computerization of consumer credit, employment, and insurance files. Data protection laws in Europe began at the individual state level, proceeded to the national level, and were followed by attempts to develop an international data protection standard. The first data protection law was enacted by the German state of Hesse in 1970.[55] The first national data protection law was enacted by Sweden in 1973.[56] France followed suit and enacted the national Law Concerning Data Processing, Files, and Liberty in 1978.[57] The Organisation for Economic Co-operation and Development (OECD)[58] made the first attempt to develop an international standard for data protection[59] with the passage of the non-binding Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines) in 1980.[60]

The Preface of the OECD Guidelines lists: "[the] development of data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers," the introduction of privacy protection legislation in over half of the OECD member countries, and the need to harmonise privacy protection legislation to ensure the free flow of information across borders as the reasons for development of the Guidelines.[61] The OECD Guidelines apply to both the public and private sectors and protect personal data that may "pose a danger to privacy and individual liberties."[62] Part two of the Guidelines define eight basic data protection principles to which member countries must adhere.[63] "The U.S. endorsed the Guidelines, but did not pass any legislation [to implement] them."[64]

The 1981 Council of Europe[65] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention) was, and is, the first and only legally binding international agreement on data protection.[66] The purpose, scope, and data protection principles of the Convention are similar to the OECD Guidelines.[67] After the implementation of the Convention, the EU began to draft a data protection Directive[68] that would harmonize the laws of its Member States to ensure the protection of the fundamental human right to privacy and the free flow of information.

3.1 DIRECTIVE OVERVIEW

The EU adopted the Data Privacy Directive on October 24, 1995.[69] Pursuant to Article 32 (1), the Directive went into effect on October 25, 1998, three years after adoption.[70] Member States were required to enact and enforce data protection laws at that national level that adhered with the principles of the Directive by the October 28, 1998 deadline.[71]

The language used in the EU Directive is consistent with the European belief that protection of personal data is a fundamental human right. The EU uses data protection rather than privacy to refer to the protection of personally identifiable

information. This is consistent with the belief in a fundamental human right to privacy because data protection is a precise term that explicitly refers to the protection of the collection, processing, storage, and dissemination of personal information.[72] In the U.S., privacy is a general term that includes data privacy in addition to many other privacy protections.[73]

The Directive defines two fundamental objectives that are similar to the objectives of the Convention and the OECD Guidelines: 1) to protect the fundamental right to privacy of individuals with respect to the processing of personal data and 2) to allow the free flow of personal data between Member States with adequate data protection.[74] The Directive also has an implied third objective that has extraterritorial implications: it requires Member States to protect the fundamental human right of privacy provided by the Directive for all personal data for every person in the EU even when the data is transferred to a third country.[75] This has particular implications for U.S. companies because the Directive mandates that data cannot be transferred to non-EU countries unless they provide "adequate protection,"[76] and it has been determined that the U.S. is among nations that do not provide "adequate protection."[77]

The Directive applies "to the processing of personal data wholly or partly by automatic means"[78] that falls within the scope of community law and that does not concern processing for public security, defense, State security, and the activities of the State in criminal law.[79] SMEs are not exempt from the Directive. All public and private sector institutions that collect personally identifiable information must comply.[80] However, a natural person processing personal data for personal or household means does not have to comply with the Directive pursuant to Article 3 (2).

3.2 THE IMPACT OF THE DIRECTIVE ON SMES

SMEs in the EU must comply with the data protection principles of the Directive. The principles of greatest concern for SMEs are the data quality and data security principles. SMEs must also be concerned with the Directive's regulation of the onward transfer of personal data to third countries and the rights of a data subject.[81] The Articles of the Directive that relate to this information are presented in the following paragraphs.

SMEs must ensure that any personally identifiable information they collect and process adheres to the principles relating to data quality. Article 6 of the Directive defines the following data quality principles:

1. Personal data must be "processed fairly and lawfully;"[82]
2. Personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;"[83]
3. Personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected;"[84]
4. Personal data must be "accurate and…kept up to date" and inaccurate data must be "erased or rectified;" [85]
5. Personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for purposes for which the data was collected."[86]

SMEs should note that Article 8 of the Directive prohibits the processing of personal data that reveals ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and that concerns health matters or sex life.[87] The Article lists exceptions in a variety of cases, including where the data subject has given explicit consent to the processing of the data, the fulfillment of employment law obligations, and processing data related to criminal offenses.[88] Processing of personal data is allowed for journalistic, artistic, and literary purposes when the right to these freedoms are balanced with the right to privacy.[89]

SMEs are required to ensure the confidentiality and security of personally identifiable information in their possession.[90] An SME should designate a person in the organization as the data controller who "determines the means of the processing of personal data."[91] Any person "who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law."[92] This ensures the confidentiality of processing. The Directive also places the controller in charge of the implementation and management of "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorized alteration, disclosure or access"[93] to ensure the security of information. The security measures put in place must be "appropriate to the risks represented by the processing and the nature of the data to be protected."[94] A controller must also ensure that any third party data processors have adequate technical and organizational security measures in place.[95] SMEs may want to implement security policies, procedures, and technology within their organizations to ensure compliance. It would also be beneficial to have regular security training to ensure that employees are knowledgeable of security policies, procedures, and technology and to perform yearly security audits to ensure continued compliance.

SMEs that engage in international commerce with non-EU nations are required to comply with Article 25 of the Directive. Article 25 prohibits the transfer of personal data to third countries for processing purposes unless the "third country in question ensures an adequate level of protection."[96] "The EU recognized that the easiest way for Member States to avoid the strictures of the Directive was to simply send their data to a third country to be processed."[97] Article 25 prevents this from occurring and forces the extraterritorial application[98] of the Directive on businesses in non-EU nations[99] who engage in business transactions with businesses in the EU. SMEs have to require that third parties in non-EU nations that they engage

in business with have an adequate level of protection. SMEs engaging in business with companies in the U.S. may perform data transfers if the companies are members of the Safe Harbor.[100] Currently, Hungary, Switzerland, U.S., and Canada are the only nations the Working Party of the European Parliament has considered to have "adequate protection."[101]

The Directive defines the rights a data subject has with respect to the processing of their personally identifiable information.[102] The Directive gives a data subject the right to notice, consent, object, access, data quality, and remedy.[103] SMEs, the data controller in particular, must ensure that these rights are protected.

The Right to Notice is defined in Article 10 of the Directive and requires that a data controller provide a data subject with the following information:

1. "the identity of the controller;"[104]
2. "purposes of the processing for which the data are intended;"[105]
3. any additional information, such as recipients of the data, existence of the right to access and the right to rectify the personally identifiable information.[106]

The Right of Consent is defined in Article 7 of the Directive.[107] In general, SMEs must obtain unambiguous consent from a data subject before they may process personally identifiable information.[108] The Directive does provide exemptions to the Right to Consent.[109]

The Right to Object is defined in Article 14 of the Directive.[110] Data subjects have the right to object to the processing of their personal information unless processing is required by national legislation. The Directive specifically states that data subjects have the right "to object…to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing purposes."[111]

Data subjects have the Right of Access to their personal information "without constraint at reasonable intervals and without excessive delay or expense."[112] Included in the Right of Access is the right of a data subject to ensure the quality of their personal information and to amend and erase personal information and block transfers of personal information.[113] The Right of Access may be restricted if the data is processed for scientific or statistical purposes and as long as the data is stored for a reasonable time.[114] Lastly, data subjects have the right to a judicial remedy "for any breach of the rights" related to data processing.[115]

SMEs may develop privacy policies that provide a data subject with notice of the information that will be collected, the uses of the information, and their rights concerning their personal information. A privacy policy should include the name and contact information of the data controller. A data subject may consent to the processing of their personal information and acknowledge receiving information about their rights concerning their personal information by signing the privacy policy.

Note that all the rights and requirements discussed in this section apply to any U.S. SME collecting or processing data within an EU Member State. This is significant because there are additional costs associated with developing and implementing Directive compliance measures. Furthermore, a U.S. SME may be subjected to fines and criminal penalties for violating Member State law by doing something that would be legal in the U.S.

4 HISTORY OF DATA PRIVACY LAW IN THE U.S.

The U.S. uses a combination of legislation, regulation, and self-regulation to protect the privacy of its citizens.[116] Historically, the U.S. has favored self-regulation over legislation and regulation to protect personal data of its citizens.[117] Federal and state data privacy legislation that has been enacted "is largely reactive as it targets specific sectors where problems have arisen."[118] This is a more fragmented and less comprehensive approach than taken by the EU. The history and culture of the U.S. provides an explanation for this fragmented approach. The U.S. was formed from a group of self-governing colonies into a federation of states.[119] The colonists' feared strong centralized governmental control,[120] so they created a democratic system of government that consisted of three branches of government with checks and balances on the powers of each branch.[121] A Bill of Rights was later added to the Constitution to addressed individual rights.[122] The colonists' fear of a strong centralized government is embedded in U.S. culture. U.S. citizens continue to have a "healthy distrust for governmental solutions."[123] This section will provide an overview of how the Constitution, torts, legislation, FTC regulation, and self-regulation all impact data privacy in the U.S. This section will conclude with an analysis of the impact of U.S. data privacy law on SMEs and advocate that SMEs should develop and implement organizational and technical data protection measures.

The U.S. Constitution does not explicitly guarantee a general right to privacy.[124] The First,[125] Fourth,[126] Fifth,[127] and Fourteenth Amendments[128] of the Constitution have been interpreted to protect the privacy of individuals from unwarranted governmental intrusion.[129] However, these amendments do not protect an individual from the actions of other citizens.[130]

The common law state privacy torts are summarized in the Restatement (Second) of Torts (Restatement).[131] These torts protect the privacy rights of individuals against infringements by private parties.[132] The Restatement includes four broadly defined[133] privacy torts:

1. an unreasonable physical intrusion upon the seclusion of another;[134]
2. the appropriation of another's name or likeness;[135]
3. unreasonable publicity given to another's name or likeness;[136]
4. publicity that unreasonably places another in a false light before the public.[137]

It must be noted that the Restatement is secondary authority that only binding in state courts that adopt the Restatement.[138] The common law state privacy torts are a matter of fifty state's laws, which vary from state to state, which is an indication of the fragmented nature of U.S. data privacy law.

Protecting the privacy of personal information first became an issue for the U.S. Congress in the 1960s and 1970s when "the consumer reporting industry was embarking on the process of computerizing its vast consumer credit, employment, and insurance files."[139] Elliot Richardson, President Nixon's Secretary of Health, Education, and Welfare, created the Advisory Committee on Automated Data Systems (Committee), a subcommittee of the Health Education and Welfare Committee, "to study the impact of computers on privacy."[140] The Committee issued a report in 1973 entitled, *Personal Data Systems: Records, Computers and the Rights of Citizens*, that outlined five principles of data protection[141] commonly known as the Code of Fair Information Practices.[142] The Committee report served as the foundation for data privacy legislation in the U.S.

There have been a number of federal laws that have been passed since the 1970s that relate to protecting personal information in the public and private sectors, for instance:

- Privacy Act 1974[143]
- Fair Credit Reporting Act of 1970[144]
- Fair Credit Billing Act of 1974[145]
- Federal Family Educational Rights and Privacy Act of 1974[146]
- Fair Debt Collection Practices Act of 1977[147]
- Cable Communications Policy Act of 1984[148]
- Electronic Communications Privacy Act of 1986[149]
- Video Piracy Act of 1988[150]
- Telephone Consumer Protection Act of 1991[151]
- Driver's Privacy Protection Act of 1994[152]
- Telecommunications Act of 1996[153]
- Health Insurance Portability and Accountability Act (HIPPA) of 1996[154]
- Children's Online Privacy Protection Act (COPPA) of 1998[155]
- Gramm-Leach-Bliley Financial Modernization Act (GLBA) of 1999[156]

The Privacy Act of 1974 applies to the federal government and protects the personal information of government employees; information collected by the Internal Revenue Service; and information collected by the Census Bureau.[157] The legislation that follows the Privacy Act of 1974 in the aforementioned list applies to the protection of data in specific industry sectors. The Federal Trade Commission (FTC) has responded to Congress's inaction in the area of data protection by protecting personal data using its powers under Section 5 of the Federal Trade Commission Act (FTCA).[158]

Despite the number of federal laws, there is no comprehensive national data privacy law similar to the EU Directive. Rather, U.S. federal laws that pertain to the protection of personal data are targeted at specific sectors where there have been particular problems. This is another indication of the fragmented nature of U.S. data privacy law.

The Federal Trade Commission has played an increasingly active role in the data privacy arena.[159] The FTC has adopted a "pro-privacy agenda [that] emphasizes both enforcement and education."[160] The FTC protects data privacy by "[guarding] against unfairness and deception by enforcing companies' privacy promises about how they collect, use and secure consumers' personal information."[161] The FTC also protects data privacy by enforcing the Gramm-Leach-Bliley Act,[162] Fair Credit Reporting Act,[163] Children's Online Privacy Protection Act,[164] and the Safe Harbor Agreement.[165] The FTC provides reports and testimonies to Congress on data privacy protection issues, initiatives, and needs in the U.S.[166] The FTC's privacy reports and testimonies since the year 2000[167] have stressed the need for federal data privacy legislation.[168]

4.1 SELF-REGULATION

The U.S. has favored self-regulation over proactive broad based national legislation to protect data privacy.[169] Self-regulation occurs when a business or group of businesses voluntarily create and adopt standardized codes of conduct for the protection of personal information.[170] The business community championed the creation of voluntary membership organizations, known as seal programs, to enforce the voluntary privacy policies of members.[171] A member of a seal program places a membership seal graphic on their web site to indicate compliance with the membership organization's policies.[172]

TRUSTe[173] and BBBOnline[174] are two of the most successful seal programs available.[175] TRUSTe "is an independent, non-profit privacy organization whose mission is to build users' trust and confidence on the Internet and, in doing so, accelerate growth of the Internet industry."[176] Member businesses that "adhere to established privacy principles and agree to comply with [TRUSTe's] oversight and consumer resolution process"[177] are awarded a TRUSTe "branded online seal, or 'trustmark,'"[178] that indicates TRUSTe compliance to their visitors. BBBOnline is a wholly owned subsidiary of the Council of Better Business Bureaus.[179] "BBBOnline's mission is to promote trust and confidence on the Internet through the BBB*OnLine* Reliability and Privacy Seal Programs."[180]

It is important to note that a privacy seal on a web site does not mean that the web site protects the privacy of the information it collects.[181] A privacy seal merely assures a visitor that the web site they are viewing has adopted a privacy policy that is in accordance with its data processing activities.[182] A web site "could post a privacy policy stating that they sell collected user information to everyone who asks, that the user has no choices or options as regards collection or sale, that there is no security on the site to speak of to protect information, and that users have no options to correct errors."[183]

Self-regulation has not been effective in the U.S.[184] In 1998, a study by Georgetown business professor Mary Culnan revealed that "only 14 percent of the Web's commercial sites were posting any sort of policy regarding the use of personal information."[185] An FTC report on online privacy of the same year "concluded that industry self-regulation was not yet effective."[186] As a result, Consumer groups pressured the federal government to intervene to ensure privacy protection.[187] In 1999, Culnan performed a follow up study and "found that 65.7 percent of web sites were now posting privacy policies."[188] However, although more web sites were posting privacy policies in 1999 than in 1998, a research study in 2000 by Annie Anton and Julie Earp "found that many online privacy policies [were] self-contradictory, incomplete, and often vaguely specified."[189] Moreover, "[Anton and Earp] identified several instances where online sites clearly stated policies that were also clearly violated, on the very same site."[190] The FTC, a prior proponent of self-regulation, changed its position in its 2000 report to Congress, calling for federal legislation to "ensure adequate protection of consumer privacy online."[191] The FTC continues to be an opponent of industry self-regulation and a proponent of federal legislation that will protect consumer privacy.[192]

4.2 IMPACT OF UNITED STATES DATA PRIVACY LAW ON U.S. SMES

Most of the federal laws that regulate privacy do not impact most SMEs because they are industry specific. No law requires an SME with purely domestic markets to adopt a privacy policy if they are not in a regulated industry. However, SMEs that choose to post a privacy policy on their company web site should note that they may face legal action under Section 5 of the FTCA[193] if their data practices do not adhere to their policy. As a result, SMEs with a privacy policy on their web site should perform annual policy audits to ensure that their data practices are in accordance with the privacy policy posted on their web site to decrease the risk of legal action.

Although SMEs in unregulated industries do not have to develop or implement data protection measures, SMEs should develop and implement data protection measures because it is a smart business practice.[194] The increasing number of computer security attacks from internal employees and external attackers[195] support that it is important for all businesses to develop and implement organizational and technical data protection measures to protect their information assets. Information drives business activity. SMEs risk significant financial loss or business failure if their information, including propriety and personal information, is stolen, copied, modified, or deleted.[196] An SME that implements data protection measures throughout their organization reduces the potential risk of loss from a data security breach. Furthermore, an SME that implements data protection measures may benefit from increased consumer confidence in their operations.[197]

SMEs may choose to develop and manage data protection measures internally or externally. Internal management of data protection measures may only be feasible for a small business with extensive financial and human capital resources. Data protection is a complex area of expertise that requires a person or persons with both organizational and technical expertise and the financial resources to purchase and install the necessary technical equipment. It may be more feasible for an SME to hire an external consultant to develop and manage data protection measures. Affordable, technical managed data protection solutions are readily available and highly recommended. However, an SME must make sure that a managed solution provider has adequate data protection measures in place to prevent access to the company's information.

In general, an SME should do the following to ensure proactive data protection:

- Classify the security levels of company information;[198]
- Define physical security perimeters and restrict access to authorized personnel;[199]
- Develop security policies and procedures and train employees on their purpose and use;[200]
- Develop a privacy policy in accordance with the Code of Fair Information Practices;
- Designate a member of the organization at a Chief Privacy Officer or Chief Security Officer to manage security breaches and privacy breach inquiries;
- Physically and technically secure all computers and computer networks within the organization;[201]
- Perform annual audits of organizational and technical data protection measures.

SMEs should consult an attorney and a security professional when developing and implementing data protection measures to ensure that adequate measures are in place.

5 THE SAFE HARBOR AGREEMENT

Although it is recommended that U.S. SMEs in purely domestic markets develop and implement data protection measures, U.S. SMEs are not required by law to do so unless they are in an industry impacted by industry specific privacy legislation. U.S. SMEs that engage in business activity in the EU are also not required to implement data protection measures. However, a company that engages in business activity with the EU, and fails to operate in a country that affords "adequate protection" of personal data, may have all data transfers into their country from the EU blocked and face fines and criminal penalties under Article 25[202] of the Directive. Since the U.S. does not have comprehensive data privacy laws, it has met the Directive's requirement of "adequate protection" impart through the development of the Safe Harbor Agreement (Safe Harbor). The Safe Harbor provides a privacy framework companies in the U.S. may comply with to meet the "adequacy" standard of the EU Directive.[203] The Safe Harbor was negotiated by the U.S. Department of Commerce (Department of Commerce) and the European Commission to bridge the gap between each nation's different approaches to data privacy.[204] The EU approved the Safe Harbor Agreement in July 2000 and the Safe Harbor became effective November 1, 2000.[205]

The Safe Harbor framework consists of seven privacy principles and fifteen frequently asked questions.[206] A Safe Harbor Workbook is given on the Department of Commerce Safe Harbor web site to help companies who volunteer to join the Safe Harbor meet the requirements of self-certification.[207] A business that chooses to self-certify to adhere to the Safe Harbor "must comply with the Safe Harbor's requirements and publicly declare that they do so."[208] Self-certification may be accomplished by sending a letter signed by a corporate officer to the Department of Commerce indicating that the business adheres to the Safe Harbor.[209] The letter should contain the name and contact information for the organization, a description of the organization's processing of personal information received from the EU, and a description of the organization's privacy policy.[210] A business must indicate their involvement in the Safe Harbor in their privacy policy.[211] A business must self-certify annually with the Department of Commerce and continue to adhere to the requirements of the Safe Harbor.[212] All companies taking advantage of the benefits of the Safe Harbor are listed on the Department of Commerce website.[213]

Enforcement of the Safe Harbor takes place in the U.S., with U.S. law, and is enforced by industry self-regulation.[214] Safe Harbor "organizations are required to have procedures for verifying compliance; to have in place a dispute resolution system that will investigate and resolve individual complaints and disputes; either independent or self-assessment; and to remedy problems arising out of a failure to comply with the principles."[215] Failure of an organization to comply with self-regulation may be actionable under the Section 5 of the Federal Trade Commission Act that declares that "unfair or deceptive trade practices affecting commerce" [216] are illegal. The U.S. Department of Transportation will also enforce the Safe Harbor for industry sectors within its jurisdiction.[217]

The following seven Safe Harbor Principles (Principles) embody the data privacy protections of the Directive:[218]

1. **Notice** – about the purposes and use for the information they collect, who to contact with inquiries or complaints, and the types of third parties who receive the information;
2. **Choice** – to opt-out of disclosing information to a third party or used for a purpose different from which it was originally collected and to opt-in for the disclosure of sensitive information to a third party or used for a purpose different from which it was originally collected;
3. **Onward Transfer** – transfers to third parties require the application of notice and choice principles and the assurance that the third party has adequate protection of the information;
4. **Access** – individuals must have access to information an organization has about them and be able to correct, amend, or delete the information;
5. **Security** – reasonable security measures must be in place to prevent loss, misuse and unauthorized access, disclosure, alteration, and destruction of personal information;
6. **Data Integrity** – personal information must be relevant for its use, reliable, accurate, complete, and current;
7. **Enforcement** – an organization must have dispute resolution, verification, and remedy systems in place;[219]

Businesses concerned about the Access Principle should be aware that they "may charge a reasonable fee and may set reasonable limits on the number of times that access request from a particular individual [may] be met"[220] within a given period. A fee and limitations on frequency of access may deter abuse of the Access Principle.[221] A business should respond to any request for access to personal information within a "reasonable time period."[222] There are instances when access to personal information may be denied;[223] however, any reasons for denying access should be specific and well documented by a business.[224]

The Safe Harbor FAQs recommend that a business use one of the following three options to satisfy the dispute resolution requirement of the Enforcement Principle:

1. "compliance with private sector developed privacy programs that incorporate the Safe Harbor Principles;"[225]

2. "compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution;"[226]
3. compliance with data protection authorities in the EU.[227]

SMEs may use private sector privacy seal programs such as the TRUSTe and BBBOnline[228] to meet the dispute resolution requirement of the Enforcement Principle.

Businesses in the Safe Harbor are encouraged to perform either data protection self-assessments or outside compliance reviews on an annual basis to ensure compliance with the verification requirement of the enforcement principle.[229] A corporate officer must sign a verification statement indicating that a self-assessment or outside compliance review has been performed.[230] "The methods of review may include without limitation auditing, random reviews, use of 'decoys,' or use of technology tools as appropriate."[231] Compliance review information should be made available to individuals upon request.[232]

6 CONCLUSION

Information technologies and the Internet threaten the privacy of personal information. Moreover, information technologies and the Internet make it easy to collect, process, store, and disseminate personal information quickly and inexpensively across national borders. The EU has taken a broad based national regulatory approach to protecting the personal information with the adoption of the Data Privacy Directive in 1995. The U.S. uses a combination of legislation, regulation, and self-regulation to protect the privacy of its citizens**.** The U.S.'s piecemeal approach to data privacy protection may have developed from the nation's cultural fear of strong centralized governmental control that stems from the founding of the nation. As a result, U.S. citizens have afforded more trust to the private sector than the public sector allowing commerce activities to occur with minimal interference.

Entrepreneurs in the U.S. and EU should be aware of the cultural differences towards entrepreneurship and data privacy laws that impact their business activities. U.S. entrepreneurs are likely to be surprised by the EU Directive's level of regulation and potential for fines and criminal penalties if data practices violate the law. However, many U.S. based SMEs are already developing and implementing privacy policies and other data protection measures to meet consumer demand and because it is a sound business practice. In developing these policies, it makes good business sense if a company has consumers and employees in the EU, to take Safe Harbor into consideration. Safe Harbor protection allows a U.S. based SME to meet the "adequacy" standard of the Directive to reduce the possibility of blocked data transfers, fines, and criminal penalties.

It is likely that more data privacy laws will be enacted in the U.S. in the near future as people become more concerned about data privacy abuses. During the 2000 election, President George W. Bush stated that he "believe[s] that privacy is a fundamental right, and that every American should have absolute control over his or her personal information,"[233] but what this means in terms of a comprehensive national privacy law has yet to be seen. SMEs in the U.S. should take a proactive approach to data privacy and immediately develop and implement organizational and technical data protection measures. Data protection measures are a smart business practice because they protect a company's proprietary information, including personally identifiable information, from being accessed, modified, or deleted by internal and external attackers with malicious intent. Moreover, proactive implementation of data protection measures will help an SME increase business by building consumer confidence and prepare them for nascent data privacy laws in the U.S.

Footnotes

[i] I would like to thank the University of St. Thomas, Bush Foundation, and Professor Susan J. Marsnik, Esq. for making this article possible. I would like to extend special thanks to Professor Marsnik, Esq. for encouraging me to write this article and for guiding me throughout the process. I also would like to acknowledge John Rossman, Esq. of Moss & Barnett, P.A. and Leslie C. Bender, Esq. for their input and assistance with this article.

[*] Bachelor of Arts in Entrepreneurship and Computer Science, University of St. Thomas, St. Paul, Minnesota

[1] Personal Interview with Professor Susan J. Marsnik, Esq., Chair of the Business Law Department, University of St. Thomas College of Business (May 27, 2003).

[2] *See* Mark Memmott and Susan Page, A Different World Dawns for Bush, USA Today, Jan. 18, 2001, available at http://www.usatoday.com/news/washington/inaug/2001-01-18-newworld.htm (last visited May 26, 2003). *See also* E-Mail from John Rossman, Esq., Attorney, Moss & Barnett, P.A., to Brian Kalis, Student at the University of St. Thomas (May 19, 2003) (on file with author).

[3] For example, personal information may be collected from public government records, including, postal address information, arrest records, divorce records, court records, property records, death certificates, marriage certificates, birth certificates, and voting records. This information may be compiled to create a comprehensive profile of a private citizen. *See* Privacy Rights Clearinghouse, From the Cradle to the Grave: Government Records and Your Privacy, at http://www.privacyrights.org/fs/fs11-pub.htm (last visited May 26, 2003); *See also* Rossman *supra* note 2; *See also* U.S.

Department of Commerce, Safe Harbor Workbook, available at http://www.export.gov/safeharbor/sh_workbook.html (last visited May 26, 2003).

[4] The EU is a European supranational governmental body that is currently composed of fifteen Member States. The fifteen Member States of the EU are Belgium, France, Germany, Italy, Luxembourg, The Netherlands, Britain, Denmark, Ireland, Greece, Spain, Portugal, Austria, Finland, and Sweden. The Treaty on European Union (TEU) enacted by the European Community on February 7, 1992 created the EU. The purpose of the TEU was to create an ever-closer union through an Economic and Monetary Union, Common Foreign and Security Policy, and intergovernmental cooperation on Justice and Home Affairs. The TEU officially came into effect on November 1, 1993. *See* Desmond Dinan, *Ever Closer Union: An Introduction to European Integration* (Neill Nugent ed., Lynne Rienner Publishers 1994) (1994).

[5] *See* Barbara Crutchfield George, Patricia Lynch, and Susan J. Marsnik, U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive, 38 Am. Bus. L.J. 735, 735 (2001).

[6] *See* Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. (L 281) 1 [hereinafter Directive].

[7] "The determination of 'adequate protection' in third countries became such an issue that a study was commissioned to test a methodology for assessing the adequacy of the level of protection of individuals with regard to processing personal data in six non-EU countries and with respect to five categories of data transfer." *See* George, Lynch, and Marsnik, *supra* note 5, at 737 n.8. *See also* Charles D. Raab et al., European Commission Tender No. XV/97/18/D, Final Report, Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer, at 38, 202 (Sept. 1998).

[8] *See* Safe Harbor Overview, at http://www.export.gov/safeharbor/sh_overview.html (last visited May 22, 2003).

[9] Personally identifiable information is information that may be used to directly or indirectly identify a person, such as "an identification number or to one or more factors of his physical, physiological, mental, economic, cultural or social identity." *See* Directive, *supra* note 6, at art. 2.

[10] *See* Safe Harbor Workbook *supra* note 3.

[11] *See* Reuters, The Privacy Dilemma in the Internet Age (Feb. 06, 2002), available at USA Today: http://www.usatoday.com/tech/tech/2001-05-09-privacy-analysis.htm, (last visited May 26, 2003).

[12] *See* Rossman, *supra* note 2.

[13] "SMEs are small, non-subsidiary independent firms, defined in the EU as employing fewer than 250 workers, and in the U.S. as fewer than 500. They account for 60-70% of total employment in most countries." *See* Alison Benney, Banking on Small Business, The OECD Observer, Winter 2000 No. 223. This article will use the SME acronym to refer to small and medium size entrepreneurial enterprises.

[14] *See* Associated Press, FBI Survey Finds Computer Attacks Up (Apr. 08, 2003), available at USA Today: http://www.usatoday.com/tech/news/2002/04/08/fbi-survey.htm, (last visited May 26, 2003).

[15] *Id.*

[16] The ten Eastern European nations that signed the Treaty of Accession to join the EU by May 1, 2004 are: Cyprus, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia, and Slovenia. European Parliament Gives Thumbs Up to EU Enlargement by Poland, 9 Other Candidates, Interfax Poland Business News Services, B.V., Apr. 10, 2003.

[17] *See* Dinan, *supra* note 4, at 191 (discussing the Copenhagen criteria for EU enlargement).

[18] *See* Donald F. Kuratko and Richard M. Hodgetts, Entrepreneurship: A Contemporary Approach Fourth Edition 672 (John Weimeister ed., Dryden Press 1998) (1989).

[19] *See Id.* at 6. *See also* Commission of the European Communities, Green Paper: Entrepreneurship in Europe, January 21, 2003 [hereinafter Green Paper].

[20] *See* David Bollier, The Global Wave of Entrepreneurialism: Harnessing the Synergies of Personal Initiative, Digital Technologies, and Global Commerce 2, The Aspen Institute (1999).

[21] *Id.* at 27.

[22] *See* Benney, *supra* note 13.

[23] *See* EOS Gallup Europe upon request of the European Commission, Flash Eurobarometer 134 "Entrepreneurship" 4 (November 2002). [herein Eurobarometer] (Survey of entrepreneurial attitudes in the EU, U.S., and EFTAN nations).

[24] *Id.* at 10-11.

[25] *Id.* at 10.

[26] *Id.* at 30.

[27] *Id.* at 47.

[28] *See* Bollier, *supra* note 20, at 6.

[29] *Id.* at 6.

[30] *Id.* at vi.

[31] *Id.* at 6.

[32] *Id.* at 7.

[33] *Id.* at 5.
[34] *Id.* at 23.
[35] *Id.* at 24.
[36] *Id*.
[37] *Id.*
[38] *Id.*
[39] *Id.* at 26.
[40] *Id.* at vi.
[41] *Id.* at 26.
[42] *Id.*
[43] *See* Eurobarometer, *supra* note 23.
[44] *See* Bollier, *supra* note 20.
[45] *Id.* at 24.
[46] *See* Eurobarometer, *supra* note 23, at 47.
[47] Some have proposed that the European belief of a privacy right developed from the abuse of personal information during WWII by the Nazis to control populations. *See* Michael W. Heydrich, A Brave New World: Complying with the European Union Directive on Personal Privacy Through the Power of Contract, 25 Brook. J. Int'l L., 417 (1999). *See also* George, Lynch and Marsnik, *supra* note 5, at 743.
[48] G.A. Res. 217, U.N. Doc A/III of 10, at Article 12 (Dec. 10, 1948) [hereinafter Declaration].
[49] Article 12 of Universal Declaration of Human Rights: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks. " *See Id*.
[50] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter Convention].
[51] *Id.*; *See also* Tracie B. Loring, An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States, 37 Tex. Int'l L.J. 421, 425 (2002).
[52] *See Id.* at 423.
[53] *See* Safe Harbor Workbook, *supra* note 3.
[54] Robert R. Schriver, You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission, 70 Fordham L. Rev. 2777, 2782 (2002). (discussing privacy legislation before the 1998 Directive). *See infra* at notes 203-233 and accompanying text.
[55] Fred H. Cate, The Changing Face of Privacy Protection in the EU and the U.S., 33 Ind. L. Rev. 173, 180 n.34 (1999); *See also* James M. Assey, Jr. and Demetrios A. Eleftheriou, The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?, 9 CommLaw Conspectus: J. Comm. L. & Pol'y 145, 150 (2001).
[56] *See* Cate, *supra* note 55, at 180; *See also* Assey and Elefheriou, *supra* note 55, at 149.
[57] *See* Assey and Elefheriou, *supra* note 55, at 149.
[58] The OECD is an organization composed of "thirty member countries sharing a commitment to democratic government and the market economy…The OECD produces internationally agreed instruments, decisions and recommendations to promote rules of the game in areas where multilateral agreement is necessary for individual countries to make progress in the globalised economy." *See* Organisation for Economic Co-operation and Development, About: OECD, available at http://www.oecd.org/EN/about/0,,EN-about-0-nodirectorate-no-no-no-0,00.html (last visited May 20, 2003).
[59] *See* Shriver, *supra* note 54, at 2782.
[60] *See* The Organisation for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, at http://www.oecd.org/EN/document/0,,EN-document-43-1-no-24-10255-43,00.html (last visited May 20, 2003) [hereinafter OECD Guidelines].
[61] *Id.* at Preface.
[62] *Id.* at Part One: General Definitions, Scope of Guidelines, 2.
[63] The eight basic principles are: 1) Collection limitation principle; 2) Data quality principle; 3) Purpose specification principle; 4) Use limitation principle; 5) Security safeguards principle; 6) Openness Principle; 7) Individual participation principle; 8) Accountability principle. *See Id.*, at Part Two: Basic Principles of National Application.
[64] *See* Shriver, *supra* note 54, at 2783; *See also* Anna Shimanek, Do You Want Milk with Those Cookies?: Complying with the Safe Harbor Privacy Principles, 26 Iowa J. Corp. L. 455, 463 (2001).
[65] The Council of Europe is an intergovernmental organization with the following aims: "to protect human rights, pluralist democracy and the rule of law; to promote awareness and encourage the development of Europe's cultural identity and diversity; to seek solutions to problems facing European society; and to help consolidate democratic stability in Europe by backing political, legislative, and constitutional reform." The Council of Europe is distinct from the EU. However, all EU Member States are also members of the Council of Europe. *See* Council of Europe, An Overview, available at http://www.coe.int/T/E/Communication_and_Research/Contacts_with_the_public/About_Council_of_Europe/An_overview/

(last visited May 20, 2003). The Council of Europe was conceptualized by Winston Churchill on September 19, 1946 and was created on May 7, 1948. *See* Council of Europe, A Short History of the Council of Europe, available at http://www.coe.int/T/E/Communication_and_Research/Contacts_with_the_public/About_Council_of_Europe/A_Short_Story/ (last visited May 20, 2003).

[66] *See* Council of Europe, Background: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, available at http://conventions.coe.int/treaty/en/Treaties/Html/108.htm (last visited May 20, 2003).

[67] The purpose of the Convention was to "secure in the territory of each Party for each individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him." *See Id.* at art. 2. The Convention covered data protection in both the private and public sectors. *See Id.* at art. 3.1. Eight data protection principles were listed in the Convention: 1) Duties of the parties; 2) Quality of data; 3) Special categories of data; 4) Data security; 5) Additional safeguards for the data subject; 6) Exceptions and restrictions; 7) Sanctions and remedies; and 8) Extended protection. *See Id.* Chapter Two.

[68] *See* Shriver, *supra* note 54, at 2783.

[69] Directive, *supra* note 6.

[70] *Id.* at art. 32.1.

[71] As of September 2002, all fifteen Member States of the EU had implemented, or were in the process of implementing, national legislation that adhered to the principles of the Directive. However, most Member States were slow to implement national legislation that adhered to the Directive by the October 25, 1998 deadline. Legal action was taken against France, Ireland, and Luxembourg to force compliance with Directive. The ten Eastern European countries that will be joining the EU on May 1, 2004 are currently in compliance with the Directive. *See* First Report on the Implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final. (provides a detailed report on the status of the implementation of the Directive by Member States).

[72] Julia M. Fromholz, The European Union Data Privacy Directive, 15 Berkeley Tech. L.J. 461, 470 (2000). (discussing the U.S. perspective on data privacy).

[73] *Id.*

[74] Directive, *supra* note 6, at art. 1.1-2.

[75] *Id.* at pmbl. 20 and art. 25.

[76] *See* George, Lynch, and Marsnik, *supra* note 5, at 737 n.8.

[77] The U.S. does not provide "adequate protection" as the Directive defines it. However, the U.S. and EU have negotiated a Safe Harbor Agreement so U.S. businesses may meet the "adequacy" standard of the Directive by choosing to adhere to the principles of the Safe Harbor. *See infra* at notes 203-233 and accompanying text.

[78] Directive, *Supra* note 6, art. 3.1.

[79] *Id.* at art. 3.2.

[80] *Id.*

[81] The Directive defines a data subject as "an identifiable natural person…who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." *See* Directive, *supra* note 6, at art. 2.a.

[82] *Id.* at art. 6.1.a.

[83] *Id.* at art. 6.1.b.

[84] *Id.* at art. 6.1.c.

[85] *Id.* at art. 6.1.d.

[86] *Id.* at art. 6.1.e.

[87] *Id.* at art. 8.1.

[88] *Id.* at art. 8.2.

[89] *Id.* at art. 9.

[90] *Id.* at art. 16-17. The Directive does not explicitly state that SMEs are required to ensure the confidentiality and security of personally identifiable information in their possession. The Directive applies to both the public and private sectors of which SMEs operate, so SMEs are required to ensure the confidentiality and security of personally identifiable information in their possession because the law applies to their operations. This paper focuses on the application of data privacy laws to entrepreneurial ventures so all information from the Directive is put in the context of SMEs.

[91] *Id.* at art. 2.d.

[92] *Id.* at art. 16.

[93] *Id.* at art. 17.1.

[94] *Id.*

[95] *Id.*

[96] *Id.* at art. 25.1.

[97] *See* Shriver, *supra* note 54, at 2785.

[98] *See* George, Lynch and Marsnik, *supra* note 5.

[99] The extraterritorial application applies to any organization in a non-EU nation that receives personal data from the EU not just businesses. This phrasing was used because this article is focused on the impact of data privacy law on SMEs.
[100] The Safe Harbor is an agreement between the U.S. and EU that allows businesses to self-certify to a set of security principles so they may meet the Directive's "adequacy" requirement. *See* Safe Harbor Workbook, *supra* note 3; *See also discussion infra* notes 203-233 and accompanying text.
[101] *See* EU Data Protection Commission, Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries, available at http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm (last visited May 21, 2003).
[102] Directive, *supra* note 6.
[103] *Id.*
[104] *Id.* at art. 10.a.
[105] *Id.* at art. 10.b.
[106] *Id.* at art. 10.c.
[107] *Id.* at art. 7.
[108] *Id.* at art. 7.
[109] Consent is not required from the data subject if processing is necessary: 1) "for the performance of the contract of which the data subject is a part or…at the request of the data subject entering into a contract;" 2) for the controller to comply with a legal obligation; 3) "to protect the vital interests of the data subject;" 4) "for the performance of a task carried out in the public interest;" 5) for the purposes of legitimate interests pursued by the controller or by third parties except where interests conflict with fundamental rights of the data subject. *See Id.*
[110] *Id.* at art. 14.
[111] *Id.* at art. 14.b.
[112] *Id.* at art. 12.1.
[113] *Id.* at art. 12.2.
[114] *Id.*
[115] *Id.* at art. 22.
[116] *See* Safe Harbor Overview, *supra* note 8.
[117] See Loring, *supra* note 51, at 426.
[118] *Id.* at 412; *See also* Heydrich, *supra* note 47, at 412.
[119] *See* Heydrich, *supra* note 47, at 412.
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] *See* Schriver, *supra* note 54, at 2778.
[124] Edward Fenno, Federal Internet Privacy Law, S.C. Law., Jan.-Feb. 2001, at 36, 28.
[125] The First Amendment "protects speech, including commercial speech, from government intrusion, thereby impacting informational privacy." The First Amendment's protection of free speech and free press allow for the free flow of information, which conflicts with data privacy protection. *See* Loring, *supra* note 51, at 427.
[126] The Fourth Amendment provides some protection from governmental intrusion upon personal privacy if an individual can demonstrate that the government has violated a "legitimate expectation of privacy." However, any information that is voluntarily entered into the stream of commerce or that is made publicly accessible to others is not protected. *See Id*. "In order to establish a 'legitimate expectation of privacy,' the individual must meet the requirements of a two-part test: (1) 'the individual, by his conduct, [must have] 'exhibited an actual (subjective) expectation of privacy'…[such that] the individual has shown that 'he seeks to preserve [something] as private'"; and (2) 'the individual's subjective expectation of privacy [must be] one that society is prepared to recognize as ''reasonable'' …[in that] 'the individual's expectation, viewed objectively, is 'justifiable under the circumstances.'" Smith v. Maryland, 442 U.S. 735, 740 (1979); *See also Id*.
[127] The Fifth Amendment affords an individual with some privacy protection because it prohibits the government from taking private property for public use without just compensation. "The Supreme Court extended the Fifth Amendment's Taking Clause in Ruckelshaus v. Monsanto Co. to protect stored data." Section 1 of the Fourteenth Amendment affords similar privacy protections to the Fifth Amendment but applies to State governments. *See* Loring, *supra* note 51, at 428; *See also* Heydrich, *supra* note 47, at 413.
[128] Section 1 of the Fourteenth Amendment affords similar privacy protections to the Fifth Amendment but applies to State governments. *See* Loring, *supra* note 51.
[129] *See* Loring, *supra* note 51.
[130] *See* Heydrich, *supra* note 47, at 413.
[131] Restatement (Second) of Torts 652 (1976).
[132] *See* Loring, *supra* note 51, at 428.
[133] *Id.*
[134] *See* Restatement (Second) of Torts, *supra* note 131.

[135] *Id.* at 652C
[136] *Id.* at 652D
[137] *Id.* at 652E
[138] *See* Heydrich, *supra* note 47, at 413.
[139] "At least six subcommittees of the U.S. Congress considered the issue of privacy during the 1960s and 1970s." *See* Simson Garfinkel and Gene Spafford, Web Security, Privacy & Commerce Second Edition 592-3 (Deborah Russell ed., O'Reilly & Associates 2002) (1997).
[140] *See Id.* at 593; *See also* Heydrich, *supra* note 44, at 414.
[141] "The report annunciated five fundamental principles with regard to an individual's right to privacy: 1) the individual's right to determine what files exist about him; 2) knowledge how information by the individual will be used; 3) requirement that the individual consent to broader use of the information that originally contemplated by the record holder; 4) right of the individual to access the files and the opportunity by him to correct outdated or incorrect information; 5) files should received adequate security and should be maintained correctly." *See* Heydrich, *supra* note 44, at 414; *See also* Garfinkel, *supra* note 139, at 593.
[142] *See* Garfinkel, *supra* note 139, at 593.
[143] 5 U.S.C. 552a (1994).
[144] Fair Credit Reporting Act, 15 U.S.C. 1681a-t (1994).
[145] 15 U.S.C. 1666.
[146] 20 U.S.C. 1232g.
[147] Pub. L. No. 95-109, 91 Stat. 874 (1977) (codified as amended at 15 U.S.C. 1692-92o (1994)).
[148] Pub. L. No. 98-549, 98 Stat. 2779 (1984) (codified as amended at 47 U.S.C. 551 (1994)).
[149] 99 Pub. L. No. 508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. 2510-22 (1994)).
[150] 18 U.S.C. 2710 (2000).
[151] Pub. L. No. 102-243; 105 Stat. 2394 (1991) (codified as amended at 47 U.S.C. 227 (1994)).
[152] Pub. L. No. 106-81, 113 Stat. 1286 (1999) (codified as amended at 18 U.S.C. 2721 (2000)).
[153] 47 U.S.C. 222 (2000).
[154] Pub. L. 104-191 (1996).
[155] 15 U.S.C. 6501-06 (2000) [hereinafter COPPA].
[156] Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. 6801-09 (2000)) [hereinafter GLBA].
[157] *See* Loring, *supra* note 51, at 2795.
[158] Section 5 of the FTCA gives the FTC the power to protect consumers from "unfair and deceptive" trade practices. The FTC has used this power in the data privacy arena. Federal Trade Commission Act, 15 U.S.C. 45(a)(1) (1999).
[159] The following statement from FTC commissioner Sheila Anthony on the FTC's Privacy Agenda confirms this: " although some companies have made a good faith effort, the private sector, as a whole, continues to fail to effectively self regulate. Absent federal legislation that sets standards to be followed by everyone, it is unlikely that consumers' privacy can be adequately protected from identity theft, commercial harassment, and hucksterism." *See* Federal Trade Commission, Statement of Commissioner Sheila Anthony on the Commission's Privacy Agenda, available at http://www.ftc.gov/opa/2001/10/antthonystatement.htm (last visited May 22, 2003).
[160] The FTC's privacy agenda consists of the following initiatives: 1) creating a do not call list; 2) beefing up enforcement against spam; 3) helping victims of ID theft; 4) putting a stop to pretexting; 5) encouraging accuracy in credit reporting and compliance with the Fair Credit Reporting Act; 6) enforcing privacy promises; 7) increasing enforcement and outreach on Children's Online Privacy; 8) encouraging consumers' privacy complaints; 9) enforcing the telemarketing sales rule; 10) restricting the use of pre-acquired account information; 11) enforcing the Gramm-Leach-Bliley Act; 12) holding workshops. *See* Federal Trade Commission, Privacy Agenda, available at http://www.ftc.gov/opa/2001/10/privacyagenda.htm (last visited May 22, 2003).
[161] *See* Federal Trade Commission: Privacy Initiatives, Introduction, available at http://www.ftc.gov/privacy/index.html (last visited May 22, 2003).
[162] *See* GLBA, *supra* note 156.
[163] *See* FCRA, *supra* note 144.
[164] *See* COPPA, *supra* note 155.
[165] *See* Safe Harbor Workbook, *supra* note 3.
[166] *See* Federal Trade Commission: Privacy Initiatives, Enforcing Privacy Promises: Reports and Testimony, available at http://www.ftc.gov/privacy/privacyinitiatives/promises_rep&test.html (last visited May 22, 2003).
[167] This was the year that a report was released that shifted the FTC's position from self-regulation to federal legislation.
[168] *See* FTC Privacy Initiatives Overview, *supra* note 161.
[169] *See* Loring, *supra* note 51, at 426.
[170] *See* Safe Harbor Workbook, *supra* note 3, at U.S. Approach to Privacy.
[171] *See* Garfinkel, *supra* note 139, at 597.

[172] *Id.*
[173] Members of TRUSTe's basic privacy program must adhere to the following principles: 1) "Adopting and implementing a **privacy policy** that factors in the goals of your individual Web site as well as consumer anxiety over sharing personal information online; 2) Posting **notice and disclosure** of collection and use practices regarding personally identifiable information (data used to identify, contact, or locate a person), via a posted privacy statement; 3) Giving **users choice and consent** over how their personal information is used and shared; 4) Putting **data security and quality, and access** measures in place to safeguard, update, and correct personally identifiable information." *See* TRUSTe, Program Principles, available at http://www.truste.org/programs/pub_principles.html (last visited May 23, 2003); TRUSTe has developed the following four self-regulatory privacy seal programs: Privacy Seal Program, Children's Seal Program, EU Safe Harbor Program, and E-Health Seal Program. A business needs to submit a privacy statement and a TRUSTe application to be considered for membership. Membership is awarded if the documents submitted meet the seal program criteria. Businesses are charged a sliding scale membership fee that is based on annual revenues. *See* TRUSTe, Frequently Asked Questions, available at http://www.truste.org/about/truste/about_faqs.html (last visited May 23, 2003).
[174] The BBBOnLine Privacy Program awards the privacy seal to businesses that have proven to meet the high standards set in the program requirements, including: 1) posting of an online privacy notice meeting rigorous privacy principles; 2) completion of a comprehensive privacy assessment 3) monitoring and review by a trusted organization; 4) participation in the programs consumer dispute resolution system. *See also* BBBOnline, Privacy Program Eligibility Requirements, available at http://www.bbbonline.org/privacy/apply.asp (last visited May 23, 2003); BBBOnline has developed the following four self-regulatory privacy seal programs: BBBOnline Privacy Seal, BBBOnline Kid's Privacy Seal, BBBOnline EU Safe Harbor Seal, and BBBOnline Japanese Privacy Seal. The BBBOnline membership application process and fees re similar in structure to the TRUSTe program. *See* BBBOnline, BBBOnline Privacy Seal, at http://www.bbbonline.org/privacy/ (last visited May 23, 2003)
[175] *See* Garfinkel and Spafford, *supra* note 139.
[176] *See* TRUSTe, Frequently Asked Questions, *supra* note 173.
[177] *Id.*
[178] *Id.*
[179] *See* BBBOnline, About Us, available at http://www.bbbonline.org/about/ (last visited May 23, 2003).
[180] *Id.*
[181] *See* Garfinkel and Spafford, *supra* note 139, at 598.
[182] *Id.*
[183] *Id.*
[184] *See* Garfinkel and Spafford, *supra* note 139, at 597; *See also* Schriver, *supra* note 54, at 2798.
[185] *See* Garfinkel and Spafford, *supra* note 139, at 597.
[186] *See* Schriver, *supra* note 54, at 2798.
[187] *See* Garfinkel and Spafford, *supra* note 139, at 597.
[188] *Id.*
[189] *Id.*
[190] *Id.*
[191] The 2000 FTC report, Privacy Online: Fair Information Practices in the Electronic Marketplace, called for federal legislation to protect the privacy of personally identifiable information collected from commercially oriented web sites. The document simplified the security guidelines set forth in the Code of Fair Information Practices to notice, choice, access, and security. *See* Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace, available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited May 23, 2003); *See also* Shriver, *supra* note 54.
[192] *See* FTC, Privacy Initiatives, *supra* note 161.
[193] *See* FTCA, *supra* note 158, at section 5.
[194] *See* Rossman, *supra* note 2.
[195] *See* Associated Press, *supra* note 14.
[196] The 2002 FBI survey respondents "said they lost at least $455 million as a result of computer crime…the most serious monetary losses came from the theft of money or proprietary information." *See Id.*
[197] *See* Steven Hetcher, Changing the Social Meaning of Privacy in Cyberspace, 15 Harv. J. Law & Tech 149, 159 (2001).
[198] The *Site Security Handbook* (RFC 2196), http://www.ietf.org/rfc/rfc2196.txt, is a resource an SME may use to assist with the classification of information and the development of security policies.
[199] *Id.*
[200] *Id.*
[201] At a minimum, an SME should have a firewall at their Internet gateway router or application firewalls on each computer in a network; use 8 character alphanumeric passwords on all systems; only allow authorized access to computer systems; and apply security patches for all computer software. Other recommendations include the following: use an Intrusion Detection

System to monitor network traffic for attacks; implement systems with redundant data to prevent data loss from natural disaster; and develop an incident response plan to prepare for response when a security incident occurs.
[202] Directive, *supra* note 6, at art. 25.
[203] *See* Safe Harbor Workbook, *supra* note 3.
[204] *Id.*
[205] *Id.*
[206] *Id.* at Description of the Safe Harbor Framework.
[207] *Id.*
[208] *Id.*
[209] *See* Safe Harbor FAQ6 – Self-Certification, available at http://www.export.gov/safeharbor/FAQ6SelfCertFINAL.htm (last visited May 21, 2003).
[210] *Id.*
[211] *Id.*
[212] *Id.*
[213] *See* U.S. Department of Commerce: Safe Harbor, Safe Harbor List, available at http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited May 21, 2003). There are current over 300 companies listed on the Safe Harbor List web page.
[214] *See* Safe Harbor Workbook, *supra* note 3.
[215] *Id.*
[216] *See* FTCA, *supra* note 158. However, it has been proposed that the FTC does not have jurisdiction because the Safe Harbor protects European citizens not U.S. citizens. The FTC was created to protect U.S. consumers, not consumers in other countries. *See* Joel R. Reidenberg, E-Commerce and Trans-Atlantic Privacy, 38 Hous. L. Rev. 717, 740 (2001).
[217] *See* Safe Harbor Workbook, *supra* note 3.
[218] *See* George, Lynch and Marsnik, *supra* note 5.
[219] *See* U.S. Department of Commerce, What do the Safe Harbor Principles Require, available at http://www.export.gov/safeharbor/sh_overview.html (last visited May 21, 2003).
[220] *See* Safe Harbor FAQ 8.9, available at http://www.export.gov/safeharbor/FAQ8AccessFINAL.htm (last visited May 27, 2003).
[221] *Id.*
[222] *See* Safe Harbor FAQ 8.11, available at http://www.export.gov/safeharbor/FAQ11FINAL.htm (last visited May 27, 2003).
[223] Research or Statistical purposes; national security; defense; or public security. *See* Safe Harbor FAQ 8.5, *supra* note 220.
[224] *Id.*
[225] *Id.*
[226] *Id.*
[227] *Id.*
[228] *See infra* notes 173-183 and accompanying text.
[229] Safe Harbor FAQ 7, available at http://www.export.gov/safeharbor/Faq7verifFINAL.htm (last visited May 27, 2003).
[230] *Id.*
[231] *Id.*
[232] *Id.*
[233] *See* Associated Press, Internet Privacy (Oct. 09, 2000), available at USA Today: http://www.usatoday.com/news/opinion/issues/internet.htm (last visited May 27, 2003). President Bush has not taken any proactive measures to protect data privacy since inauguration. In fact, the passage of the U.S. Patriot Act and similar legislation has reduced personal privacy protection and has legalized increased governmental intrusion of personal privacy in the guise of protecting the nation during the War on Terror.