PRIVACY IN THE DIGITAL AGE: FACT OR FICTION?

May 2010

Author:
Dr. John H. Nugent, LLM, CPA, CFE, CFF, CISM, FCPA
Associate Professor
School of Management
Texas Woman's University
Denton, TX
Email: jnugent@twu.edu
Phone: 001-214-682-8025

Important Note: The opinions expressed in this paper are solely those of the author and not necessarily those of the institution that employs him.

Table of Contents

PRIVACY IN THE DIGITAL AGE: FACT OR FICTION?

Abstract: This paper examines the history, drivers, issues, and various legal approaches to protecting privacy (unified and sector) with a focus on the United States, and to a large degree on data privacy. A determination is made whether either approach affords the individual privacy in the digital age. The paper examines specific risks as well as fundamental challenges facing the privacy paradigm.

"…even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of the right."[1] *William Beaney*

"…government exists for man, not man for government."[2] *Justice William O. Douglas*

I. History of Privacy, Drivers, and the Modern Communication Infrastructure

Privacy has been a concern of mankind throughout the millennium. In written documents as recorded in the Code Hammurabi, it can be seen that as early as 1760 B.C., the Babylonian Empire made it a

[1] Beaney, William M. 1966. "The Right to Privacy and American Law," 31 Law & Contemporary Problems, pp. 254 – 255. This journal article was published following the landmark U.S. Supreme Court decision in *Griswold v. Connecticut,* 381 U.S. 479. 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965) 59-60.

[2] Douglas, W. 1958. The Right of the People. Doubleday, N.Y., N.Y. p.87.

crime to break a hole through the wall of another's house.[3] As Soma indicates, this Code also required individuals receiving goods or money as a custodian to keep such a transaction a secret.[4]

Socrates also defended himself in court by demonstrating that he 'privately' versus 'publicly' instructed students who were free to accept or reject his words.[5] Soma goes on to show that in 1361, The Justices of the Peace Act in England provided for the arrest of 'peeping Toms' and 'eavesdroppers'.[6]

From ancient times in the Orient, we see the terms 'saving face' and 'losing face' used in the lexicon in dealing with maintaining one's 'public' status, persona, or reputation; or conversely, the losing of such status or position by being 'publicly' embarrassed or humiliated. It has been said in the Chinese culture that such public embarrassment is "worse than losing all of one's savings."[7]

In certain other cultures we see the right of 'Honour Killings' where family members have been permitted to kill other family members that have brought shame upon the family essentially representing a loss of face.[8]

---

[3] Soma, J. and Rynerson, S. 2008. Privacy Law. Thomson/West Publishing. P.8. This treatise is an excellent volume that addresses the many legal, economic, and social issues regarding privacy.
[4] Supra at 3, p. 8.
[5] Supra at 3, p.9. See also http://www.sacred-texts.com/cla/plato/apology.htm for a translation and articulation of Socrates defense.
[6] Supra at 3, p.9.
[7] See the Foreign Policy Association page for a brief discussion of the importance of 'saving face'.
http://www.fpa.org/newsletter_info2484/newsletter_info_sub_list.htm?section=The%20Issue%20of%20Saving%20Face
[8] For a short educational piece on 'Honour Killings' please see:
http://www.gendercide.org/case_honour.html

In the 1800's the political philosopher John Locke warned that the state should not invade, and in fact should be constrained from invading the property or person of its citizens.[9]

The Romans and British long held that 'a man's home is his castle'.[10] Essentially this means that no one should interfere with another in the privacy of one's home. This premise was incorporated into U.S. law as well in the form of numerous Amendments to the U.S. Constitution.[11]

These views of privacy throughout the years highlight that privacy exists on a number of planes: individual to individual, individual to a group or an enterprise of one form or other, an individual to a government, etc. Such varied relationships have demonstrated the challenges in defining, protecting, maintaining, and regulating privacy in complex interconnected societies.

Whitman points out that divergent sensibilities lie at the base of how the U.S. and Europe view privacy, and this may be the cause

---

[9] Locke, J. 1887. "Two Treatises of Government." 204. George Routledge & Sons, 2nd ed. A presentation of these works may be viewed online at : http://www.lonang.com/exlibris/locke/

[10] "A Man's Home is His Castle" - This saying is as old as the basic concepts of English common law. From the "Morris Dictionary of Word and Phrase Origins" by William and Mary Morris (HarperCollins, New York, 1977 and 1988)."You are the boss in your own house and nobody can tell you what to do there. In 1644, English jurist Sir Edward Coke (1552-1634) was quoted as saying: 'For a man's house is his castle, et domus sua cuique tutissimum refugium' ('One's home is the safest refuge for all'). First attested in the United States in 'Will and Doom' (1692). From "Random House Dictionary of Popular Proverbs and Sayings" by Gregory Y. Titelman (Random House, New York, 1996). See http://www.phrases.org.uk/meanings/an-englishmans-home-is-his-castle.html

[11] The Fourth Amendment to the U.S. Constitution limits the right of search and seizure while Fifth and Fourteenth Amendments limit the reach of eminent domain – the ability of a government to take one's home.

of the divergent approaches to addressing this issue.[12] Here Whitman indicates a higher degree of focus in Europe on the concern for public dignity, while in the U.S., a higher degree of focus on the "citadel of individual sovereignty."[13]

Such basic insights by leading persona and bodies over the years concerning privacy leads one to question if there is some deeper, basic driver in each of us that compels a need for privacy.

Here, Maslow demonstrated in his 'Hierarchy of Needs Satisfaction' Model that humans have a range of needs from the most essential (Level 1) to the more lofty (Level 5) that they are driven to satisfy.[14]

Table 1: Maslow's Hierarchy of Needs

Level	Type of Need	Examples
1	Physiological	Thirst, sex, hunger, survival
2	Safety	Security, stability, protection
3	Love and Belongingness	To escape loneliness, love and be loved, and gain a sense of belonging
4	Esteem	Self-respect, the respect others
5	Self-actualization	To fulfill one's potentialities

[12] Whitman, J. 2004. "The Two Western Cultures of Privacy: Dignity versus Liberty" Yale Law Journal, Vol. 113, p. 1162

[13] Supra at 12

[14] Maslow. 1954. *Motivation and Personality*. *This treatise established five levels of human needs. Maslow shows that the lowest level needs first need to be satisfied in the main before moving to higher levels of needs satisfaction. The model may be viewed online at:* http://pareonline.net/getvn.asp?v=5&n=11

In Maslow's model, the most basic of human needs; thirst, sex, survival, safety, food, and shelter drive fundamental human behavior. In humans, the endocrine system and hypothalamus are the elements that control many auto response activities including, but not limited to:

- Hunger, Thirst, Sex Drive
- Fear, Flight, Fight, Survival Responses
- Moods
- Sleep
- Blood Pressure

basically, those functions that deal with Maslow's most basic needs.[15] Hence, this inherent and innate concern for privacy may lie at the core of what people experience bio-chemically as basic fear/survival/security/safety and higher level needs. That is, individuals may have a bio-chemical foundation to not want private information divulged in a manner that may 'harm' or 'embarrass' them, and this state may be governed by our glands and hormones in an unconscious and somewhat involuntary manner.

Clearly, nations hold such a collective belief relative to a nation's secrecy laws that require much 'private' information not be divulged to those not 'cleared' or to enemies of the state as such dissemination may be harmful or embarrassing to the nation. Such a national perspective may just be a collective manifestation of the individual's bio-chemical compulsion for privacy, i.e.; fear, survival, security, and safety as well as higher level needs fulfillment requirements.

[15] Hadley M. and Levine J. 2007. Endocrinology. 6th ed. Pearson Prentice Hall. See this volume for a presentation on the function of the hypothalamus gland and the endocrine system.

In the final analysis, privacy involves a range of behavior from total personal anarchy to a situation where the right to act is weighed against the rights of others.[16] It is in developing this accepted line of behavior that we have difficulty in defining precisely what privacy is. As part of this dynamic, U.S. Supreme Court Justice William O. Douglas wrote that Justice Brandies:

> …wanted to put the individual and the individual's privacy first, and to establish only the controls that would keep the individual from being regimented.[17]

Whatever the driver(s), virtually everyone values their privacy to a degree - similar to many and unique to some.

In times past, prior to modern transport, mail and communications systems, privacy was easier to maintain. That is, privacy was often time sensitive as private information was often not written down nor was it easily accumulated, disseminated, or retrievable and usually required physical proximity in order to compromise it.

However, as soon as taxes began to be collected and census taken, privacy was beginning to erode and persons were becoming traceable through written records. And as technology and systems matured, we see the beginnings of widespread readings of others' mail and the tapping of telegraph systems.[18] Such erosion of

---

[16] Doyle, C. and Bagaric M. 2005. International Journal of Human Rights, Vol. 9, No.1, pp.3-36,p.27.

[17] Glancy, D. 1981. "Getting Government off the Backs of People: The Right of Privacy and Freedom of Expression in the Opinions of Justice William O. Douglas," Santa Clara Law Review, Vol. 21, p.1050.

[18] Huitric, E. 2000. "Timeline: Privacy in America." Web publication. This chronological piece may be seen at: http://issuu.com/sciam/docs/extended-privacy-

privacy has continued with the discovery of the uniqueness of fingerprints and DNA, and with the introduction of social security numbers or national I.D. cards in the U.S. and other countries respectively, as well as via digital technology and the Internet.

It was the invention and market introduction of the Kodak Instant Camera which some posit caused Warren and Brandeis to publish their now foundational piece, "The Right to Privacy" in the Harvard Law Review.[19] Here the authors called for a new tort regarding one's 'right 'to be let alone'.[20] In this article, these authors coined the term 'invasion of privacy'. They expressed their strong opinion that one's basic 'right to be let alone' is the most fundamental and far reaching of rights and the right most valued by man. Their suggested method of protecting such a right to be let alone was a tort action. As will be seen, tort is but one approach to addressing privacy matters.

As Lloyd points out regarding the principle of 'the right to be let alone':

> In terms of isolation from scrutiny of others, the average individual living in a town or city enjoys vastly more personal privacy than did our ancestors living in small

---

timeline/3?mode=embed&documentId=080905202111-362202d8bd0b48319813a4aac215b34c&layout=grey

[19] Friedman, L. 2004. Private Lives: families, individuals and the law, p. 147. Harvard University Press. Others claim the genesis of this piece lies in the publication of the details of a party the Warren family held.

[20] Warren, S. and Brandeis L. 1890. "The Right to Privacy." Harvard Law Review. Vol. 4, No. 5. 193. A copy of this journal article may be viewed at: http://www.lawrence.edu/fast/BOARDMAW/Privacy_brand_warr2.html. The term "right to be let alone" first appeared in 1834. The U.S. Supreme Court stated that a "defendant asks nothing — wants nothing, but to be let alone until it can be shown that he has violated the rights of another." *Wheaton v. Peters*, 33 U.S. 591, 634 (1834).

> villages where every action was known to and a source of comment for neighbours.[21]

Lloyd may have this exactly correct. But now, through on-line social networks, instant communications, and a relationship of '1 to ALL' (The Internet) where communications are digitally recorded for posterity both locally and in the network or in large databases, we may have come full circle, digitally speaking, to Lloyd's proposition of relative privacy being community based. It is that now the community is unbounded by time and geography and has an unforgiving memory. That is, community today is anywhere and everywhere and communications are recorded and available all the time to those 'connected'.

Today, with modern mail, transport, and communications systems, communication is near immediate and almost seamless. We have phones with cameras and computers with video cams and integrated speakers. Close to 2 billion of the approximately 5 billion people on the planet will soon be interconnected via the Internet.[22] The Internet has established a communication environment that is basically a 'One to All' network – essentially, everyone has the ability to be in everyone else's home or private space electronically. Moreover, communications and business transactions take place nearly at the speed of light. This electronic network has essentially voided the typical privacy protection mechanisms of 'borders and trust'. That is, by interconnecting to

[21] Lloyd, I. 1997. Information Technology Law, 2nd ed. Butterworths., pp. 28-29.
[22] The ITU estimates over 1.5 billion Internet users in 2008. The U.S. Census Bureau estimates over 2 billion Internet users by 2015. http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom99.html.

the Internet individual borders and trust have essentially been extended and granted to all others so connected. Essentially, we have opened the door for other parties to digitally trespass into our private space whether intended or not. Moreover, as so much personal information today is accumulated, aggregated, and amalgamated in repositories held by others, our private living rooms now are located electronically in numerous domains, many of which may be totally unknown to us. Hence, via modern communication and computer systems, the world to a degree may have electronically regressed into an electronic 'small village' where each may know much about the other, and where a time insensitive record of such personal actions and knowledge is maintained.

This 'One to All' environment has coincided with the digitization of our persona and economic wealth. We are now digital beings and are represented by digital avatars, dossiers of ourselves, and our wealth is represented by 1s and 0s and is reachable electronically from almost anywhere.[23]

Robert Metcalfe, the acclaimed 'Father of the Ethernet,' has postulated that the value of the network increases at an exponent of the numbers of nodes connected to it.[24] It is likely that risk is increasing at an even higher exponent. This belief is based on the almost multitude of daily reports in the press of compromises of 'private' information via digital abuses.[25]

---

[23] Solove, D. 1972. The Digital Person. New York University Press, pp. 27-55.
[24] For a definition of Metcalfe's Law please see: http://www.yourdictionary.com/telecom/metcalfe-s-law
[25] "A Chronology of Data Breaches. 2005 to 2009." Privacy Rights Clearinghouse. http://www.privacyrights.org/ar/ChronDataBreaches.htm#2009. This site lists data

IDC estimates that 161 exabytes of data were created in 2006, or 3 million times the amount of information contained in all the books ever written with the number expected to rise to 988 exabytes by 2010, just a year away.[26] And Cisco reports that it expects Internet traffic to reach 667 exabytes annually by 2013, or approximately 56 exabytes a month.[27] Never before has so much data been available to so many with virtually no checks and balances as to the access, accuracy, distribution, use, or knowledge of the true ownership of such data.

II. Definitions of Privacy

Privacy is generally regarded by many as:

> …the expectation that confidential personal information disclosed in a private place will not be disclosed to third parties, when that disclosure would cause either embarrassment or emotional distress to a person of reasonable sensitivities. *Information* is interpreted broadly to include facts, images (e.g. photographs, videotapes) and disparaging opinions.[28]

However, there is no uniformity of opinion as to exactly what the definition of privacy is or should be.

---

breaches that have compromised personal data files on over 260,000,000 parties in just a four year period. Of course this list contains only those reported incidents.

[26] An exabyte is 10^{18} bytes or 1,000,000,000,000,000,000 bytes. Gantz, J. (March, 2008). "An Updated Forecast of Worldwide Information Growth Through 2011." This paper is available via the EMC Corporation website at: http://www.emc.com/digital_universe/

[27] The Cisco Visual Network Index (VNI). Report may be viewed at: http://www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html

[28] Standler, R. 1977. "Privacy Law in the USA." Please see: http://www.rbs2.com/privacy.htm

Solove recants that "privacy suffers from an embarrassment of meanings."[29] Moreover, he demonstrates that new technologies are challenging 'privacy' in very challenging ways.

Basically, we see various approaches to defining this term exist. The first, being an interpretative approach (including those who are thought to legislate from the bench) based on statutory or case law and practice. A second approach based on perhaps a more philosophically pure manner of developing a definition is based on the underlying principles and concepts of privacy. A third more narrowly defined approach proscribes a 'control' perspective.

As Soma indicates, one class using the 'control' approach to defining privacy defines it as "limited access to the self."[30] Here this class indicates that interferences or invasions of the self may be further defined based upon interferences with "personal information, secrecy, repose, reserve, bodily integrity, anonymity, solitude, and seclusion." [31] But then these parties differ in defining what these postcedents mean.

A leading professor of public policy, David O'Brien, states that a weakness in the "limited access to the self" definition is that one does not necessarily choose whether another has access to one's

[29] Solove, D. 2006. "A Taxonomy of Privacy." University of Pennsylvania Law Review 154, pp 477-564.
[30] Supra at 3, p.17
[31] Supra at 3, p. 17

personal information.[32] That is, one does not always control access to or use of one's personal information, especially in the digital age.

Professor Fried of Harvard University and Alan Weston of Columbia University have both weighed in on the 'control' approach to defining privacy as well.[33] Fried suggests that privacy:

> … is not simply an absence of information about us in the minds of others: rather, it is the control we have over information about ourselves.[34]

And Westin posits:

> Few values so fundamental to society have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists.

He goes to define privacy as:

> ...Privacy is the claim of individuals, groups, or

---

30 O'Brien, D. 1979. Privacy, Law, and Public Policy. Praeger, Westport, Conn, pp. 3-31.

33 For a detailed examination of the 'control' issue regarding privacy, please *See* Westin, A. 1967. PRIVACY AND FREEDOM (defining information privacy as the claim of "individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"); Fried, C. "Privacy", 1968. 77 Yale Law Journal, pp. 475 - 482 ("Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves."); Gormley, K. 1992. " One Hundred Years of Privacy," Wisconsin Law Review, pp. 1335- 1356 ("Control of information about oneself is critical in determining how and when (if ever) others will perceive us, which is in turn essential to managing our individual personalities."); Posner, R. "Privacy", *supra* note 5, at 104 ("Economic analysis of the law of privacy . . . should focus on those aspects of privacy law that are concerned with the control by individuals of the dissemination of information about themselves."); Schauer, F. 1998. "Internet Privacy and the Public-Private Distinction", 38 Jurimetrics Journal, pp. 555 – 556. ("The privacy interest addressed here is the power to control the facts about one's life.").

34 Fried, C. 1968. "Privacy." Yale Law Journal, pp. 475-482.

> institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[35]

Basically, Westin is defining privacy as a property right. This too may be indicated in the Chinese interpretation that losing one's reputation is worse than losing one's savings.

Conceptual definitions such as the 'right to be let alone' are also problematic as they are subject to broad interpretation as to what the term means.

We also see differences in the definition and intent of privacy depending on whether U.S. Constitutional, common, or statutory law applies. As Farlex indicates:

> The meaning of the term *privacy* changes according to its legal context. In constitutional law, privacy means the right to make certain fundamental decisions concerning deeply personal matters free from government coercion, intimidation, or regulation. In this sense, privacy is associated with interests in autonomy, dignity, and self-determination. Under the common law, privacy generally means the right to be let alone. In this sense, privacy is associated with seclusion. Under statutory law, privacy often means the right to prevent the nonconsensual disclosure of sensitive, confidential, or discrediting information. In this sense, privacy is associated with secrecy.[36]

Compounding this definitional issue is an analysis by Professor Judith Thomson. Thomson's analysis indicates that virtually all privacy rights' issues may be addressed by looking to other

[35] Westin, A. 1967. Privacy and Freedom. New York: Atheneum
[36] Farlex. The Free Dictionary. This definition may be viewed at: http://legal-dictionary.thefreedictionary.com/Privacy+rights

remedies under the law such as for trespass, misappropriation, invasion, surveillance, etc.[37] She infers that the 'right to be let alone' as a definition is both too broad and too narrow. That is, in her opinion there is significant overlap with laws in other areas with remedies already established in these other regimes. Hence, privacy matters are already addressed in the law and need not be addressed separately.

The legislative approach in the U.S. often results in contradictory interpretations and legislation from the bench based on similar sets of facts. In the case of the United States, the U.S. Constitution does not even contain the word 'privacy.' However, many jurists have interpreted different sections of the U.S. Constitution to infer privacy rights. This will be examined further under the Sectoral approach component of this paper.

The varied meanings and definitions of privacy have confounded attempts to develop a single unified definition of privacy. As we have seen legal privacy has been defined as the right to be let alone, the right to control information about oneself, and having the attribute of limited accessibility.[38] Allen demonstrates that privacy has been used as an umbrella term encompassing: "solitude, seclusion, confidentiality, secrecy, anonymity, data protection, data security, fair information practices, modesty, and reserve."[39]

---

[37] Thomson, J. 1975. "The Right to Privacy." Philosophy and Public Affairs, Vol.4, No. 4, pp. 295-314. A copy of this journal article may be retrieved at: http://www.eecs.harvard.edu/cs199r/readings/thomson1975.pdf

[38] Allen, A. 2007. Privacy Law and Society. Thompson West, p.5.

[39] Supra at 38, p5.

One scholar, Simon Davies, has concluded:

> Privacy is a generic definition label for the grab bag of values and rights, to arrive at a general definition of privacy would be no easier today than finding a consensus on a definition of freedom.[40]

Hence, at the foci of the issues regarding privacy, we see a fundamental issue in defining what precisely privacy means.

III. Organization of Economic Cooperation and Development (OECD)

With much forethought and prognostication, the OECD realizing the impact technology was having and was likely to have on privacy and data security, served as the pioneer organization in promulgating multinational guidance on what member nations and others should address in order to protect their citizens' private information going forward. The OECD looked to the 1948 U.N. Declaration on Human Rights in establishing its privacy guidance.[41] This pioneering work was far ahead of its time as viewed in relation to the awareness or availability of the Internet to most.[42]

---

[40] Davies, S. 1997. Re-engineering the Right to Privacy: How Privacy has been Transformed from a Right to a Commodity." Technology and Privacy: The New Landscape, pp. 143-153. Paper may be purchased from ACM at: http://portal.acm.org/citation.cfm?id=275289

[41] For the text of the 1948 UN Human Rights Declaration please see: http://www.un.org/en/documents/udhr/

[42] For a timeline of important events in the history of the Internet, please see: http://www.netvalley.com/archives/mirrors/davemarsh-timeline-1.htm

In 1980 the OECD issued a set of guidelines that has served as the basis for much of the legislation, regulation, and policy we have today regarding privacy and the protection of personal data.[43]

Following the lead by the OECD, many organizations and countries today have developed laws and regulations that govern the collection, control, storage, use, dissemination, and destruction of personal information. The common elements found in these laws and regulations address the following matters:

- Ownership, collection, use, reproduction, transmission, and destruction of databases or elements thereof
- Ownership, control, and use of database networks
- Ownership, control, and use of communications networks
- Ownership, collection, aggregation, control, use, reproduction, movement, or destruction of content
- Outsourcing the production or management of applications or any of the elements described above
- Marketing of applications or uses of privacy data.

IV. Unified Approach – The European Union

In Europe taking its lead from the OECD and the move to unify Europe itself, The Council of Europe and its member states such as

[43] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, issued 23 September, 1980. This document may be viewed at: http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html This work was the outgrowth of a convocation called by the OECD in 1977. In its final form it only consists of 77 paragraphs, but is comprehensive and far sighted in its nature.

the United Kingdom chose a unified approach to protecting one's private data.

Council of Europe's Directive 95/46/EC and B. the UK's Data Protection Act of 1998:[44]

In 1998 there was a harmonization of privacy policy activity regarding personal information and data security. In this year The Council of Europe issued Directive 95/46/EC, and the United Kingdom issued its Data Protection Act of 1998. These promulgations synchronized major European efforts regarding the protection of privacy data.

The EC Directive established a founding principle:[45]

> In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

It can be seen here that the EC understood the issues with defining the term privacy per se, and sought instead first to establish a paradigm that addressed one's privacy rights only as it related to personal identifying data or the processing of personal information. Today, all EU members have embodied the EU Directive into national law.[46]

---

[44] Please see the following link for the complete text of the Directive at http://www.cdt.org/privacy/eudiective/EU_Directive_.html

[45] Please see: http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_1

[46] As of 2005 all EU Member States had embodied the EU Directive into national law. However, the EU filed suit in 2005 against several member nations (Germany and Austria for example) claiming improper adoption.

By focusing on privacy primarily as it related to data, the EU circumvented many of the issues we see in the U.S. today regarding privacy.

However, in other matters regarding privacy, there are quirks in EU member country laws as well. One example here is that:

> …certain continental governments assert authority to decide what names parents are permitted give to their children - a practice affirmed by the European Court of Human rights as recently as 1996.[47]

A. The UK's Data Protection Act[48] adopted the principles established in the EC Directive and was also specific to define data and its control, use, and the export of privacy data from the UK to non-European (non Council of Europe) parties.

The EU and UK Safe Harbor provisions were deemed necessary as trade with significant trading partners outside of the EU was material and would continue. Moreover, as the U.S. Privacy Protection Study Commission pointed out in the 1970s:

> …neither law nor technology now gives an individual the tools she needs to protect her legitimate interests in the records organizations

---

http://www.hunton.com/files/tbl_s10News%5CFileUpload44%5C12063%5CEC_Data Directive.pdf See also http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm for a current listing of the current status of member states.

[47] Whitman, J. 2004. "The Two Western Cultures of Privacy." The Yale Law Review, Vol. 113, p. 1158.

[48] For the full body of this UK Directive please see: http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

keep about her… [49]

it was deemed a requirement to have a Safe Harbor mechanism in place for personal data leaving the UK and EU in transit to the U.S. and other jurisdictions.

The Safe Harbor provision has been operational since November 2000 when the U.S. Department of Commerce opened the on-line self certification process for U.S. organizations.[50] The Safe Harbor mechanism provides for a voluntary process whereby U.S. entities providing adequate protection over personal data transferred to them from the EU is recognized by the Commission as providing adequate protection for the transfer of personal data under the terms of the Directive.

In the U.S., The Federal Trade Commission is primarily responsible for enforcing the Safe Harbor provision. A full list of companies that have signed up to the Safe Harbor regime can be found on the U.S. Department of Commerce's Safe Harbor website.[51]

The EU and member states approaches' to establishing a framework and principles regarding data privacy makes sense. It is a top down approach that establishes bright lines for all such that each knows what is permitted and what isn't. This approach also

[49] Soma, J. et al. 2004. "An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The U.S./EU E-Commerce Privacy Safe Harbor." Texas International Law Journal, Vol. 39, p.183.
[50] For a complete view of the Safe Harbor Agreement requirements please see the following site: http://www.export.gov/safeharbor/eu/eg_main_018365.asp
[51] For a complete list of U.S. companies participating in the Safe Harbor program, please see: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

establishes roles, responsibilities, and penalties regarding private information.

V. Sector Approach to Data Protection and Privacy – The United States

Unlike Europe where a harmonization and unified approach has been taken relative to privacy and to data protection via the guidance initially provided by the OECD Principles and subsequently by the Council of Europe Directive 95/46/EC, the U.S. has taken a sector approach to such, with many different and often disparate pieces of legislation dealing with different aspects and parties. Such a sector approach makes compliance often difficult and lacking in transparency of intent. As Glancy has pointed out in an analysis of privacy and the Internet:

> The three main characteristics of United States privacy law help to explain why it can be difficult to understand how privacy law intersects with the Internet. First, United States privacy law is diverse. Second, United States privacy law is decentralized. Third, United States privacy law is dynamic. As privacy law has evolved over the past century or so, these characteristics have resulted in a myriad of specific privacy laws applicable in the United States.[52]

To paraphrase the words of the late Chief Justice of the U.S. Supreme Court, Justice Rehnquist: "privacy laws in the U.S. defy categorical description."[53]

---

[52] Glancy, D. 2000. "At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet." 16 Santa Clara Computer and High Technology Law Journal 357, May, p.2.
[53] Supra at 52, p.2.

In the United States, states have employed common law and specific statutes to protect privacy rights through the application of four invasion of property torts: namely;

- Intrusion
- Publication
- False Light
- Misappropriation

A) The Intrusion Tort

The American Law Institute's Restatement (Second) of Torts, § 652B states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.[54]

The Restatement specifies the right to privacy is invaded by:

1) unreasonable intrusion upon the seclusion of another, as stated in 652B, or
2) appropriation of the other's name or likeness, as stated in 652C; or
3) unreasonable publicity given to the other's private life, as stated in 652D, or
4) publicity that unreasonably places the other in a false light before the public, as stated in 652E.[55]

---

[54] The American Law Institute's Restatement (Second) of Torts. For a copy of this text, please see: http://cyber.law.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm

[55] Allen, A. 2007. Privacy Law and Society, p. 33.

The most famous and founding case regarding intrusion was *Pavesich v. New England Life Insurance Co*. 122 Ga. 190, 50 S.E. 68 (Ga. 1905). In this case, Mr. Pavesich brought a tort claim of intrusion against the New England Life Insurance Company as it used his pictures in their advertisements without his permission, thereby implying he had bought insurance from them.

In this case the court upheld for Pavesich:

> The liberty which he derives from natural law …embraces far more than freedom from physical restraint. … Liberty includes the right to live as one will, so long as that will does not interfere with the rights of another or the public. One may desire to lead a life of seclusion, another may desire to lead a life of publicity; still another may wish to live a life of privacy as to certain matters…. All will admit that the individual who desires to lead a life of seclusion cannot be compelled, against his consent, to exhibit his person in any public places unless such exhibit is demanded by the law of the land.

The Pavesich case has stood the test of time and has served as the guiding law even in jurisdictions without privacy statutes. This case however raises issues for today where many join online social networking groups and post their resumes, bios, pictures, and sometimes intimate details on the web. Hence the question begs, have such actions made these people 'public' versus 'private' persons and thereby have they forfeited a basic privacy right by so doing?

Prosser informs that:

> …the tort of intrusion upon the plaintiff's solitude or seclusion is not limited to a physical invasion of his

> home or his room or his quarters. The principle has been carried beyond such physical intrusion and extended to eavesdropping upon private conversations by means of wire tapping and microphones.[56]

Hence the principle of invasion extends beyond the domain of one's physical location.

However, the intrusion tort does have limitations. In *Desnick v. ABC*, 44 F3d 1345 (&t Cir. 1995) the federal court held for ABC in determining under the facts in this case that ABC's First Amendment rights of free speech precluded claims of intrusion and trespass. That is, the public's right to know certain matters may outweigh the right of one's privacy.

B) The Publication Tort

The American Law Institute's Restatement (Second) of Torts § 652D: Publicity Given to Private Life states:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that:
>
> a) would be highly offensive to a reasonable person, and
> b) is not of legitimate concern to the public.[57]

Illustrative of the Publication Tort is the case of *Melvin v. Reid*, 112 Cal. App. 285 (Cal. Ct. App. 1931) (superseded by statute). In this

[56] Prosser, W. 1964. Torts 3rd. ed., p.832. See also "Privacy" 48 California Law Review, 383, pp. 388-89, 1960.
[57] The American Law Institute's Restatement (Second) of Torts, supra at 47.

case, the plaintiff, Melvin, years before had been charged and acquitted of a crime. Years later defendant Reid made a movie of the plaintiff presenting her past life. In this movie the defendants not only used the plaintiff's maiden name at the time she was charged, but also advertised the movie presently with both her maiden and current married name. Here the court held for the plaintiff finding that the plaintiff's maiden name could be used as it was part of a public court record. But years later to tie her past to her current married name causing her harm and loss of reputation, was actionable.

In other cases where parties had been involved in past crimes, the courts have held their privacy was not invaded as these were matters of public record and of legitimate interest to the public.[58]

C) The False Light Tort

The American Law Institute's Restatement (Second) of Torts § 652E: Publicity Placing Person in False Light states:

> One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if;
>
> a) the false light in which the other was placed would be highly offensive to a reasonable person, and
> b) the actor had knowledge of or acted in reckless disregard as to the falsity of the published matter and the false light in which the other would be placed.

[58] Please see the cases of: *Sidis v F-R Pub. Corp*, 113 F.2d 806 (2d Cir. 1940), *Briscoe v. Reader's Digest Ass'n*., 4 Cal. 3d 529 (Cal. 1971), and *Cox Broadcasting Corp. v. Cohn* 420 U.S. 469 (1975) for the application of law regarding this tort.

Here in *Lovgren v. Citizens First Nat'l. Bank*, the bank placed an ad for Lovgren's property in the local papers stating Lovgren was selling it at public auction.[59] The bank held the mortgage to the property and wanted it sold to satisfy the mortgage. No mortgage foreclosure proceedings had taken place before the ad appeared. Lovgren sued for violation of his privacy rights under False Light. The court held for Lovgren. Here it found Lovgren had no knowledge of a sale and hence the ad was false. The court next determined that the bank's action would be highly offensive to a reasonable person thereby meeting one of the tests established by the requirements of the tort of False Light.

In the case of *Lake v. Wal-Mart* Stores, Inc., however, the court on appeal determined that it did not recognize false light as it was too similar to the claims that could be made for defamation of character.[60] So in some jurisdictions, a claim under False Light may not be successful.

D) The Appropriations Tort

The American Law Institute's Restatement (Second) of Torts § 652C: Appropriation of Name or Likeness states:

> One that appropriates for his own use the name or likeness of another is subject to liability to the other for invasion of his privacy.[61]

[59] *Lovgren v. Citizens First Nat'l. Bank*, 126 Ill. 2d 411 (Ill.) (1989).
[60] *Lake v. Wal-Mart Stores, Inc*. 582 N.W.2d 231 (Minn. 1998)
[61] The American Law Institute's Restatement (Second) of Torts, supra at 47.

In *Castro v. NYT TV* the court held that TV footage shot regarding medical treatment in a medical facility with patient signed authorizations was not done for commercial purposes.[62] Hence their claim of wrongful appropriation was found to be without merit because there was no commercial profit or advantage.

In *Felsher v. University* of Evansville it was held that the university could not be successful under the privacy tort for wrongful appropriation as only people, not institutions, were covered by this tort.[63]

In the *New York Times Co. v. Sullivan* the court established that actions must be reconcilable with the Constitution's First Amendment protections and should bar press liability for false reports unless it can be shown the publisher knew the matter to be false or acted in reckless disregard of the truth.[64]

Two additional areas where a privacy tort action may be taken involve the Publicity Tort and Breach of Confidentiality Tort.[65]

E) The Publicity Tort

The right of publicity tort was developed to protect the business and commercial interests of celebrities and famous parties relative to their

[62] *Castro v. NYT TV, 370 N.J.* Super 282 (N.J. Super. Ct. 2004).
[63] *Felsher v. University of Evansville*, 755 N.E.2d 589 Ind. 2001)
[64] *New York Times v. Sullivan*, 376 U.S. 254, 284- Allen, A. supra at 95 (1964)
[65] The Publicity Tort and The Breach of Confidentiality Tort are in addition to those commonly addressed in The American Law Institute's Restatement (Second) of Torts § 652. Supra at 57.

identities (names, likeness, etc.) as such have economic value that might be taken for wrongful gain or exploitation.[66]

A case representative of this publicity tort right is that of *Carson v. Here's Johnny Portable Toilets*.[67] In this case another party began using the slogan by which the TV actor Johnny Carson had become known and associated. Carson, the actor, did not want his name or the slogan by which he had become known associated with a toilet product. The party using the slogan 'Here's Johnny Portable Toilets' admitted in his deposition that be believed other parties would associate the actor with his toilet product and thereby afford him commercial exploitation and gain from his actions. On appeal the court found for Carson because the perpetrator knew and believed others would make the association between his product and the actor.

F) The Breach of Confidentiality Tort

The Breach of Confidentiality Tort involves the claim of one party violating the trust and confidence of another. This breach usually involves a professional party such as a doctor, lawyer, accountant, hospital, clergyman, etc. that steps outside the privacy relationship and tells another of the confidential matter. In numerous U.S. states, a statute exists that addresses this breach.

In the case *Doe v. Evans* a priest was involved in counselling a couple regarding some marital difficulties.[68] During this process the priest

[66] Allen, A. supra at 55, p. 131.
[67] *Carson v. Here's Johnny Portable Toilets,* 698 F. 2d 831 (6th Cir. 1983)
[68] *Doe v. Evans*, 814 So. 2d 370, 373-75 (Fla. 2002)

developed a plan to make the couple divorce. In the process of counselling the parties, the priest became sexually active with the wife being counselled. Here the court held the priest violated his fiduciary responsibility as well as his requirement to treat confidentially the information provided by the plaintiffs. Moreover, the priest was also responsible for the resultant harm flowing from this breach.

Hence it can be seen that tort actions regarding privacy have to meet several strict parameters under the six classes or privacy torts cited above, are sometimes in conflict with statutory stipulations, and are often trumped by Constitutional imperatives.

G) The U.S. Constitution[69]

As was mentioned earlier, no where in the U.S. Constitution does the word 'privacy' appear. This condition has left open the door for broad interpretation of constitutional components by the judiciary as to whether these constitutional components do or do not provide for 'privacy' protections.

In the previous section of this paper dealing with torts, the primary focus was the individual or non-governmental party invading or violating another's privacy right. With the Constitution, we are concerned with protections from government perversion or interference of our privacy rights. To bring a claim of infringement under the Constitution, a state organ must be the intruder.

[69] For a complete copy of The Federalist papers, the U.S. Constitution, the Bill of Rights, and The Declaration of Independence, please see http://federali.st/

Preceding the actions leading to the ratification of the U.S. Constitution making it the law of the land, significant resistance to its acceptance and passage was being realized, particularly in New York. In this regard, several leading founders of the U.S.; Alexander Hamilton, John Jay, and James Madison penned a series of some 85 essays under the name 'Publius' between 1787 and 1788 which appeared in The New York Times. These papers put forth the reasons and needs to ratify the U.S. Constitution as drafted, sans the 'Bill of Rights'.

The Federalist papers put forth the reasoning for a tri-part government (executive, legislative, and judiciary) and further spelled out a set of limited powers to be bestowed to the government with all other powers left to the states or people. Since this period, the courts have often referred to The Federalist papers in interpreting the Constitution. In fact, The Federalist papers through the year 2000 have been cited by the U.S. Supreme Court 291 times in its decisions.[70]

> Chief Justice John Marshall in *Mc-Culloch v. Maryland,*[71] ...wrote that *The Federalist* was "entitled to great respect [by courts] expounding the Constitution." Moreover, he wrote in *Cohens v. Virginia* (1821): "[*The Federalist*] is a complete commentary on our Constitution, and it is appealed to by all parties in the questions to which that instrument gave birth." Ever since the founding period, lawyers, judges, politicians, and scholars have used *The Federalist* to guide their decisions about issues of constitutional government.[72]

[70] Chernow, R. 2004. Alexander Hamilton. Penguin Books, p. 260.
[71] *McCulloch v. Maryland*, 17 U.S. 316 (1819)
[72] Mervin. D. 2006. U.S. History Encyclopedia. Please see http://www.answers.com/topic/federalist-papers

In The Federalist No. 78, Hamilton makes the point that there is no need to amend the Constitution with a 'Bill of Rights' as the proposed Constitution's language protecting liberty amounts to a bill of rights; and in Federalist 84, he wrote that if such rights were explicitly enumerated, later this list would be deemed to be the only rights intended for the people.[73]

Federalist No. 84 is important in another respect. That is, in this writing Hamilton also sets forth the doctrine of 'judicial review' by federal courts regarding federal law and executive acts. This perspective gave the courts the check and balance function over the other two branches of government.

The U.S. Constitution to date has 27 amendments; the first ten of which are known as the 'Bill of Rights'.[74]

So it is these foundational documents that have established by interpretation and penumbras (shadows or emanations), that the government only has certain proscribed rights, with 'ALL' other rights being for the states and the people. Hence, the Constitution and 'Bill of Rights' has been interpreted to describe the rights of each party by proscribing what rights the federal government specifically has, with all other rights being reserved for the states and people.

[73] The Federalist No. 78 and 84 at supra 69.
[74] Please see supra 69 for a complete copy of the U.S. Constitution and Amendments thereto.

With this understanding, the court has taken great leeway in interpreting and applying the rights granted to each party under the Constitution.

As Allan indicates,[75]

> The breadth of constitutional "privacy" rights has been tested in the U.S. through distinctly contemporary debates – about abortion, sexual orientation, the right to die, and the use of surveillance technology, for example.

In the main, we see privacy matters in the U.S. guided by the First, Second, Third, Fourth, Fifth, and Fourteenth Amendments to the Constitution.

> **1) The First Amendment states**:
>
> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.[76]

On its face, it appears that such rights defined in this amendment and others are absolute. In fact, Justice Douglas makes this precise point in *Doe v. Bolton*, wherein he writes:

> First is the autonomous control over the development and expression of one's intellect, interests, tastes, and personality. These rights are

[75] Allan at supra 55, p. 183.
[76] Supra at 69.

> protected by the First Amendment and, in my view, they are absolute, permitting no exceptions…[77]

However, the courts have tempered these rights in numerous areas and ways based on the needs of others including the state and public.

The First Amendment is often in conflict with the rights of one party versus another. Here we often see conflicts between the press and the public's right to know, and the individual's right to privacy.

An illustrative case demonstrating the application of this amendment may be found in *Prince v. Massachusetts*.[78] In this case the Court held that privacy of religion is not absolute, and a minor child could not be made to distribute Jehovah Witnesses' pamphlets in contravention of state child labor laws. Here the court indicated that religion is not a license.

In another case involving the Mormon religion, *Reynolds v United States*,[79] where polygamy is a foundational element of that religion, the Court held that the government may not interfere with private religious beliefs or opinions, but it could interfere with its practices, such as the taking of a second wife, which under the laws of the U.S. is not allowed.

---

[77] *Doe v. Bolton*, 410 U.S. 179 (1973)
[78] *Prince v. Massachusetts*, 321 U.S. 158 (1944). The cases presented under the section headed The U.S. Constitution are far from complete. Rather, they are representative examples of certain aspects of these amendments as the court has applied such to privacy matters.
[79] *Reynolds v. United Sta*tes, 98 U.S. 145 (1878)

In yet another decision, the Court found in *Meyer v. Nebrask*a,[80] a case involving school segregation issues, that parents have no absolute constitutional right to send their children to schools free from government regulation. The court indicated that states have an expressed power to regulate schools.

In *Stanley v. Georgia*,[81] a case involving the search of one's residence for 'book' making (gambling) material, the police and state officials found no gambling evidence, but did find video tapes deemed to be obscene. The Court found that the right to receive information or ideas, regardless of their worth, is fundamental to being free, and except in very limited situations must be free of government intervention.

In *Brandenburg v. Ohio*, we see the Court declare that the freedom of speech is supreme so long as it is not 'directed to inciting or producing imminent lawless action."[82]

So the right to free speech, religion and other protected elements of the First Amendment have been tailored by facts and circumstances over the years. This has been particularly apparent in the numerous cases involving the right of the press to publish 'private' details of 'public' persons. As Whitman states, "The law will not work 'as law' unless it seems to the people to embody the basic commitments of their society."[83] That is, the court will continue to interpret the Constitution in tempo with the times and current perceived norms.

---

[80] *Meyer v. Nebraska*, 262 U.S. 390
[81] *Stanley v. Georgia*, 394 U.S. 557 (1969)
[82] *Brandenburg v. Ohio*, 395 U.S. 444 (1969)
[83] Whitman, supra at 11

2) The Second Amendment states:

> A well regulated Militia being necessary to the security of a free State, the right of the people to keep and bear Arms shall not be infringed.[84]

It is interesting to note the grammar and syntax of this amendment. We have an awkward fragmented introductory phrase followed by a complete but passive sentence. This has confused many. Basically, two interpretations of this amendment exist in the main, one that anyone may own and bear arms (a privacy right), and a second, that the states may form militias such as the National Guard which have the right to bear arms.

In *State v. Williams*, the Court declared, "Citizens have a constitutional right to bear arms under federal and state constitutions."[85]

The above view has prevailed, albeit with restrictions on certain types of weapons.

3) The Third Amendment states:

> No Soldier shall, in time of peace, be quartered in any house without the consent of the Owner; nor in time of war, but in a manner to be prescribed by law.[86]

---

[84] Supra at 69.
[85] *State v. Williams*, 158 Wn.2d 904, 148 P.3d 993 (Wash. 2006)
[86] Supra at 69.

In a scarcely used privacy application of this amendment regarding one's house, certain correctional officers were removed from their residential quarters located close to a correctional facility. These officers paid rent for these quarters. In a strike at the facility, the correctional officers were removed from their quarters to make room for National Guardsmen. The correction officers who had been removed from their quarters sued. The Court found for the corrections officers and stated:

> …that property-based privacy interests protected by the Third Amendment are not limited solely to those arising out of fee simple ownership but extend to those recognized and permitted by society on lawful occupation or possession with a legal right to exclude others…[87]

While the Third Amendment right to privacy has not often been invoked, the above case provides clear insight as to how the court may likely decide future cases. However, had the situation been a much larger national emergency, for instance a dirty bomb being detonated in a populated area, the court may well have found that such condition met the 'manner prescribed in law'.

4) The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation,

[87] *Engblom v. Carey*, 677 F.2d 957 (2d Cir. 1982)

> and particularly describing the place to be searched, and the persons or things to be seized.[88]

Two of the often most cited amendments in U.S. jurisprudence are the Fourth and Fourteenth amendments.

The Fourth Amendment to the Constitution is becoming the principal legal guidance in the U.S. governing privacy. Litigation relying on the guidance of the Fourth Amendment protections is enormous, with precedents going in multiple directions. Concerning data privacy, this Amendment is all important.

As can be seen above, this Amendment has as its foundation the concept of security in one's home, papers, requires reasonableness (a balancing of interests), and warrants. In fact, it has been posited that the rights subsequently protected under this Amendment were the genesis of the American Revolutionary War. It has been recounted that James Otis, Jr., a Boston attorney defending Boston merchants, argued against two onerous provisions of British law; namely general warrants and writs of assistance which provided British authorities the right to trespass on private property in search of traitorous writings or smuggled goods. Otis argued:

> Now one of the most essential branches of English liberty, is the freedoms of one's house. A man's house is his castle; and while he is quiet, he is as well guarded as a prince in his castle. This writ, if it should be declared legal, would totally annihilate this privilege.[89]

[88] Supra at 69.
[89] Kerr, O. 2009. "The Case for the Third-Party Doctrine." Michigan Law Review, Vol. 107, p. 571.

Numerous important cases in this regard reflect the application of this Amendment, and some of these applications clearly conflict with one another.

One troublesome interpretation involves the Third Party Doctrine. That is, does privacy subsist if one conveys private information to another even in the confines of one's home? This doctrine has had significant impact regarding bank information, telephone carrier information regarding subscribers, and Internet Service Providers (ISPs). That is, whose information does one's private information belong to? Does private information conveyed to another remain private? Do your bank records belong to you or the bank? In this age of electronic commerce and communications, the ramifications of this doctrine can have a tremendous far reaching impact on jurisprudence and privacy in the United States. We see this specifically in the *Hepting v. AT&T* case(s). Here, Hepting sued AT&T over the issue of warrantless wireless taps provided to the U.S. Government by AT&T.[90] Soon after this case commenced, AT&T altered its customer use policy such that certain information on its network constituted its business records, not its customers. And it now declared it was free to do what it would with this data. This policy change was likely in response to this lawsuit.[91]

[90] *Hepting v. AT&T Corp.*, No. 06-17132 and *Hepting v. United States* No. 06-17137. See also http://www.wired.com/threatlevel/2008/08/eff-and-feds-ba/

[91] Please see this article for an analysis of AT&T's change to its customer use policy. http://arstechnica.com/old/content/2006/06/7110.ars.

As, Solove states, "the third party doctrine is based on an incorrect 'conception of privacy,' a conception of privacy as total secrecy."[92] Posner concurs in stating, "…that the *Miller* line of cases is unrealistic. Informational privacy does mean refusing to share information with everyone."[93] He continues, "… one must not confuse solitude with secrecy." And Colb supports this thinking in stating, "…treating exposure to a limited audience as identical to exposure to the world" fails to recognize the degrees of privacy.[94]

In a leading case, *Boyd v. United States*, the Court used a conservative interpretation.[95] Here the government sought Boyd's personal papers in order to prove its case. The Court held:

> The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach farther than the most the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employees [sic] of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property.

In *Olmstead v. United States*, we see the Court start to chip away at the absoluteness of the protections laid down in Boyd.[96] In Olmstead

---

[92] Supra at 89, p. 571.
[93] Supra at 89, p. 571
[94] Supra at 89, p. 571
[95] *Boyd v. United States*, 116 U.S. 616 (1886)
[96] *Olmstead v. United States*, 277 U.S. 438 (1928)

the Court determined that wiretapping did not constitute search and seizure as "no entry of the houses or [offices] of the defendants" had taken place.[97] In dissenting, Justice Brandeis, stated:

> The Framers of the Constitution conferred, as the Government, *the right to be let alone* – the most comprehensive of rights and the right most valued by men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of the facts ascertained by such intrusion, must be deemed a violation of the Fifth.

In *Katz v. United States*, where the FBI had tapped a public pay phone that Katz used to send wager information, the Court held that this information was not properly obtained as no warrant had been obtained, and it further declared, "The Fourth Amendment protects people not places."[98] This case holds tremendous importance today regarding the Internet and personal mobile communications.

In 2001 in *Kyllo v. United States*, an agent of the Department of the Interior used thermal technology to determine a suspect was growing marijuana in his home as marijuana and the heat lamps used to grow it generate excessive heat.[99] The agent did not have a warrant. Here the Court found that it needed to take the long view, and while no physical penetration of the home was employed, nevertheless the surveillance "…is a search…" and is unreasonable without a warrant.

---

[97] Supra at 89.
[98] *Katz v. United States*, 389 U.S. 347 (1967)
[99] *Kyllo v. United States*, 533 U.S. 27 (2001)

Clearly, the Fourth Amendment will be used regarding data privacy invasions going forward within the United States. It should be remembered that the Constitutional protections regarding privacy only apply to governmental intrusion, not intrusions by non-governmental parties. Hence as will be discussed later, we see such commercial data repositories of vast amounts of personal data as held by ChoicePoint and Accurint growing exponentially.

5) The Fifth Amendment states:

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.[100]

As the Court demonstrated in *Kastigar v. United States*, the Fifth Amendment privilege against compulsory self-incrimination is well established.[101] Here the Court declared the Fifth Amendment:

> …protects against disclosures that witness reasonably believes could be used in a criminal prosecution or could lead to other evidence that might be so used.

[100] Supra at 69.
[101] *Kastigar v. United States*, 406 U.S. 441 (1972)

6) The Fourteenth Amendment states:

> All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.[102]

The case of *Griswold v. Connecticut*[103] is important in Constitutional law as Justice Douglas writing for the majority reaffirmed the right to privacy and indicated that privacy was "implicit in many specific provisions of the Bill of Rights."[104] This case involved the right of a Center to distribute contraceptive devices and Connecticut's law prohibiting such. This same statute made those facilitating such distribution also a party to the illegal act. Griswold, a medical director, distributed such contraceptive devices. Griswold was fined under the Connecticut statute and sued.

Justice White, concurring in the decision stated, "In my view this Connecticut law as applied to married couples deprives them of 'liberty' without due process of law."[105]

It was in *Whalen v. Roe* where the Court had to decide a case based on the collection, storage, and dissemination of information in

---

[102] Supra at 69.
[103] *Griswold v. Connecticut*, 384 U.S. 479 (1965). It was in this case that the founding principle of a "Zone of Privacy" was established with this zone originating in the penumbras or emanations (also described as shadows) of the Bill of Rights.
[104] Soma, J. 2008. Privacy Law, p. 60.
[105] Supra at 103.

government databases concerning dual use prescription drugs.[106] Here the Court established "…two branches of information: informational privacy and privacy-autonomy."[107] The Court stated:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of wealth, and social and security benefits, the supervision of public health, the direction of the Armed Forces, and the enforcement of criminal laws all require great quantities of information much of which is personal in character and potentially embarrassing or harmful if disclosed.
>
> We therefore need not, and do not decide any question which might be presented by the unwarranted disclosure of accumulated private data – whether intentional or unintentional or by a system that did not contain comparable security provisions. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.

Whalen is important in U.S. jurisprudence because it strikes at the heart of those who advocate defining privacy solely as 'one's control over his private information'. For in Whalen we see one's inability to 'control' his personal information is far from absolute.

H) Federal Statutes – The Sectoral Approach Continues[108]

In addition to U.S. Constitutional law where we have seen direction and redirection, and bright and not so bright lines drawn, the U.S.

[106] *Whalen v. Roe,* 429 U.S. 589 (1977)
[107] Soma, J. 2008. Privacy Law, p. 65.
[108] The following federal statutes are presented in chronological order.

Government has initiated numerous federal statutes in an attempt to further regulate information and privacy. In this regard, a number will be reviewed at a high level as delineated below.

1) **Freedom of Information Act of 1966 -** 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048[109]

This law was passed in order to establish transparency in government. Here the public may request Executive Branch information of an unclassified nature. If personal information is contained in the information requested, the agency makes a determination as to whether such a release would violate privacy laws. If there is a difference in opinion over this matter between the requester and the executive Branch component, a court must decide the issue. Long delays are typically incurred in receiving requested information.

2) **The Bank Secrecy Act of 1970 -** 31 U.S.C. 5311-5314e[110]

The purpose of this Act was to make it easier for the government to detect money laundering or illegal funding activities. Here financial institutions are required to report certain transactions to the U.S. Treasury. Today, this function is overseen by FinCEN.[111]

3) **The Fair Credit Reporting Act of 1970 -** 15 U.S.C. § 1681[112]

Just as the Bank Secrecy Act is about institutions having to disclose information to the government, this Act is directed at keeping certain information private. This Act defined

[109] The full text of this law is available at:
http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm
[110] The full text of this Act may be downloaded in pdf format at:
http://www.fincen.gov/statutes_regs/bsa/
[111] For a complete description of FinCEN activities, please see:
http://www.fincen.gov/
[112] The full text of this Act in pdf may be downloaded at:
http://www.ftc.gov/os/statutes/fcra.pdf

entities that collect and report such credit information on individuals as Credit Reporting Agencies (CRAs) and laid down rules regarding what may be reported as well as providing for certain consumer rights. As will be seen with other such repositories, U.S. Government agencies have 'Blanket Purchase Agreements' with these entities in order to assist in carrying out investigations as this information is deemed public source information. Hence, no warrant is required to obtain such data.

This Act was amended in 2003 by the Fair and Accurate Credit Transactions Act of 2003 which added elements principally concerning rights and protections involved with identity theft.[113]

4) Family Education Rights and Privacy Act of 1974 - 20 U.S.C. § 1232g; 34 CFR Part 99[114]

This act is to protect student information. Under 18 years of age, parents may have access to such information. Once 18, the right is the student's only. Schools may give out certain information such as name, address, date of birth, phone number, etc, but must give notice to the student. Any such student may opt out of the release of such information. Students have a right to correct erroneous information. Releases of information to other parties such as educational regulators, accreditors, etc. is permitted.

5) The Privacy Act of 1974 - 5 USC § 555[115]

This Act was passed to …protect private, personally identifiable information in federal records from being disclosed. It also mandated protections over the use of social security numbers and required the government to obtain consent before releasing personally identifiable

[113] For a complete copy of this Act, please see: http://www.treasury.gov/offices/domestic-finance/financial-institution/cip/pdf/fact-act.pdf

[114] The full text of this Act may be viewed at: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[115] For a complete copy of this Act, please see: http://www.usdoj.gov/opcl/privstat.htm

information. This law only addressed government records, not non-government records.

6) The Right to Financial Privacy Act of 1978 - 12 U.S.C. §§ 3401-342. [116]

This Act principally deals with notice being required to be given to parties when the government seeks that parties' financial information. However, no such notice is required when the institution is presented with a valid warrant. Certain carve outs also exist where non-explicitly individual identification exists or where a court order requires notice not be given until after the information sought is provided to the government.

7) The Cable Communication Protection Act of 1984 - 47 USC Sec. 551[117]

Cable operators under this Act are to protect subscriber information and not provide it to third parties. If cable operators seek to provide it to a third party, it must provide the subscriber and opt out opportunity. Cable companies are required to provide subscriber information to the government under a legitimate warrant, but not what content was watched information. It should be noted no such provision exists for ISPs regarding government requests relative to sites visited.

8) The Computer Fraud and Abuse Act of 1986 - 18 USC 1030[118]

The purpose of the Act was to address the hacking of …computer systems, in particular government computer systems, and to make such actions federal computer-

[116] For an excellent analysis of this Act, please see: http://epic.org/privacy/rfpa/
[117] The full text of this Act may be viewed at: http://epic.org/privacy/cable_tv/ctpa.html
[118] The full text of this Act appears at: http://www.panix.com/~eck/computer-fraud-act.html This Act was amended in 1986, 1994, 1996, by the USA PATRIOT Act in 2001, and in 2008 by the Identity Theft Enforcement and Restitution Act. Specifically, Section (b) of the latter Act makes punishable wrongful doers and conspirators.

related offenses. The Act governs cases with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, or where interstate or foreign commerce is involved.

9) The Electronic Communication Privacy Act of 1986 - 18 U.S.C. § 2510-22. [119]

This Act addresses the information communicated via telephone companies, ISPs, or banks. It defines such communications as falling into three classes: Subscriber Information (name address, IP address, payment method, etc.); Transaction Records (what number communicated with what number or address, time and duration of the communications, etc.); and Content Data (the actual information communicated).

The Act permits the obtaining of Subscriber Information without notification with a legitimate subpoena. In order for the government to obtain Transaction records it must present a court order showing the sought information is needed in an ongoing criminal investigation.

For Content Data, the rules are stricter. Here a 180 day rule applies, as well as a rule regarding whether the communication is stored or in transit. For electronic data stored less than 180 days and unopened, the government must provide a search warrant showing cause that a crime has been committed and the communication evidences such. The subscriber must be notified of the information sought, but prosecutors with permission of the court may delay notification under certain conditions. For communications over 180 days and unopened, the government may use either a subpoena or warrant to retrieve the communication.

The difference between transmitted (live) data and stored data is principally a moot point. For example, while certain

[119] A copy of this Act may be accessed via the following web link: http://www.it.ojp.gov/default.aspx?area=privacy&page=1285

laws make illegal the intercept of 'live' emails during transmission, stored emails may be viewed for instance by an employer. But virtually all emails become 'stored' within milliseconds of transmission.

10) The Video Privacy Protection Act of 1986 - 18 U.S.C. § 2710[120]

The Act prohibits video service providers from disclosing personally identifiable information (such as names, addresses, videos watched or rented, etc.) except in certain, limited circumstances. As a general rule, personally identifiable information may only be disclosed with the prior written consent of the individual or by warrant, subpoena, or court order.[121]

11) The Driver's Privacy Protection Act of 1994 - 18 U.S.C. § 2721 et. seq. (Public Law 103-322) [122]

This Act requires a …State department of motor vehicles, and any officer, employee, or contractor, thereof, shall not knowingly disclose or otherwise make available to any person or entity personal information about any individual obtained by the department in connection with a motor vehicle record.[123]

---

[120] For important extracts from this Act, please see http://www4.law.cornell.edu/uscode/18/2710.html

[121] The driver for enacting this measure arose as a result of Judge Robert Bork, the 1987 Supreme Court nominee, having his family's list of 146 video tapes the Bork family had previously rented from their neighborhood store disclosed by a Washington, D.C. newspaper.

[122] For a complete copy of the Act, please see: http://www.accessreports.com/statutes/DPPA1.htm

[123] One of the drivers behind this Act's coming into being was the Czechoslovakian Intelligence Service had representatives sit outside the CIA headquarters video recording all license plates on cars entering that facility. The Czehch service then purchased a directory from the Commonwealth of Virginia that contained the names and addresses of all license plate holders.

12) Communications Decency Act of 1996 (The Act was Title V of the Telecommunications Act of 1996) [124]

The Act imposed …broadcast-style content regulations on the open, decentralized Internet and severely restricted the first amendment rights of all Americans. This Act was strongly opposed by many groups because it threatened the existence of the Internet as a means for free expression, education, and political discourse.

The U.S. Supreme Court struck down the anti-decency provision of this Act in 1997 based on violations of First Amendment rights to free speech.[125] The Act thus became null and void.

13) Child Pornography Prevention Act of 1996[126]

The Act prohibited …any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture that is, or appears to be, of a minor engaging in sexually explicit conduct, or which shows any sexually explicit image that was advertised, promoted, presented, described, or distributed in such a manner that conveys the impression it depicts a minor engaging in sexually explicit conduct.

The Supreme Court struck down this Act in 2002 in *Ashcroft v. Free Speech Coalition* for being overly broad.[127]

14) Economic Espionage Act of 1996[128]

This Act …criminalizes: 1) the misappropriation of trade secrets (including conspiracy to misappropriate trade secrets and the subsequent acquisition of such misappropriated trade secrets) with the knowledge or

---

[124] For a complete copy of The Telecommunications Act of 1996 and Title V, please see: http://www.fcc.gov/Reports/tcom1996.txt
[125] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997)
[126] For a complete copy of this Act, please see: http://www.politechbot.com/docs/cppa.text.html
[127] *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002)
[128] For a complete copy of this Act, please see: http://www.tscm.com/USC18_90.html

intent that the theft will benefit a foreign power, or 2) the misappropriation of trade secrets related to or included in a product that is produced for or placed in interstate (including international) commerce, with the knowledge or intent that the misappropriation will injure the owner of the trade secret.

15) Health Insurance Portability and Accountability Act of 1996[129]

This Act has two components. The first protects parties and their families' health insurance coverage when changing employment or providing for health coverage maintenance if they have lost their employment. The second component addresses the protection of electronic medical information. Security mechanisms were to be in place by 2003.[130]

16) Child Online Protection Act of 1998[131]

This Act was to restrict access by minors to any material defined as harmful to such minors on the Internet. The U.S. federal courts have ruled that the law violates the First Amendment constitutional protection of free speech. As of 2009, the law remains unconstitutional and unenforced.

17) Gramm-Leach-Bliley 1999 (Pub. L. 106-102)[132]

This comprehensive GLB Act repealed partially the Glass-Steagall Act which had prohibited commercial

[129] For a complete copy of the Act, please see: http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf

[130] Differences in compliance actions regarding HIPAA vary widely. For example, IBM Corporation terminated health insurance companies from providing coverage to its employees if those companies would not agree to stop using social security numbers as employee identifiers. At the other end of the spectrum, students studying under an NSA sponsored CAE IA program as late as 2008 undertook 'war driving' tests in a major U.S. city. These students determined many doctors' offices electronic records are not secured. Another test was run at major U.S. city large hospitals. In these tests the word 'shalom' was found to be a password for at least one individual in each major hospital.

[131] For a complete copy of the Act, please see: http://www.ftc.gov/ogc/coppa1.htm

[132] For a complete copy of the Act, please see: http://banking.senate.gov/conf/

banks, investment banks, and insurance companies from having common ownership. Another section of this Act established privacy and security rules that financial institutions must follow. One such requirement is that financial institutions must annually tell customers in writing what personal information is collected about them and what the institution may do with that information. Customers are to be provided an 'opt out' facility.

18) U.S. Patriot Act 2001 (Public Law Pub. L. 107-56)[133]

This Act …greatly increases the reach of law enforcement agencies in the search of telephone, e-mail communications, medical, financial, and other records; … expands the Secretary of the Treasury's authority to regulate financial transactions…. The act also expands the definition of terrorism to include domestic terrorism.[134]

National Security Letters (NSLs) – a provision of the U.S. Patriot Act.[135]

Through NSLs the FBI can compile vast dossiers about innocent people and obtain sensitive information such as the web sites a person visits, a list of e-mail addresses with which a person has corresponded, or even unmask the identity of a person who has posted anonymous speech on a political website. The provision also allows the FBI to "gag" anyone who receives an NSL from telling anyone about the record demand. The Justice Department's Inspector General has reported

[133]For a complete copy of the Act, please see: http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:

[134] As an example of the scope change under this Act, subsequent to its enactment, law enforcement today only needs one warrant that now covers the entire U.S.; versus previously having to obtain warrants in each jurisdiction. This is particularly important when tracking wireless communication users. For capsule overview please see: http://en.wikipedia.org/wiki/USA_PATRIOT_Act

[135] Please see the American Civil Liberties Union (ACLU) site for a complete information on NSLs at:
http://www.aclu.org/safefree/nationalsecurityletters/index.html

that between 2003 and 2006, the FBI issued nearly 200,000 NSLs. The inspector General has also found serious FBI abuses of the NSL power.[136]

The ACLU challenged this Patriot Act statute in court in three cases. The first, called *Doe v. Holder*,[137] involves an NSL served on an Internet Service Provider. In September 2007 a federal court struck down the entirety of the National Security Letter (NSL) provisions of the Patriot Act. Judge Victor Marrero of the Southern District of New York ruled that the NSL statute's gag provisions violate the First Amendment and the principle of separation of powers. In December 2008, the U.S. Court of Appeals for the Second Circuit upheld this decision in part, finding the portions of the statute violated the First Amendment; specifically the sections that wrongly placed the burden on NSL recipients to challenge gag orders; narrowly limited judicial review of gag orders; and required courts to defer entirely to the executive branch. The appeals court also ruled that the government must now justify the more than four-year long gag on the "John Doe" NSL recipient in the case.

The second case, called *Library Connection v. Gonzales*, involved an NSL served on a consortium of libraries in Connecticut. In September 2006, a federal district court ruled that the gag on the librarians violated the First Amendment and the government ultimately withdrew both the gag and its demand for records.[138]

The third case, called *Internet Archive v. Mukasey*,[139] involved an NSL served on a digital library. In April 2008, the FBI withdrew the NSL and the gag as part of the settlement of a legal challenge brought by the ACLU and the Electronic Frontier Foundation.[140]

---

[136] Supra at 135.
[137] *Doe v. Holder* No. 04-2614 (S.D.N.Y. June 18,2009) (dkt. no. 167)
[138] Supra at 135
[139] *Internet Archive v. Mukasey* (No. 07-6346-CW (N.D. Cal))
[140] Supra at 135.

19) The Federal Information Security Management Act of 2002 (44 U.S.C. § 3541**)** [141]

This FISMA Act requires government agencies to implement security programs, policies, and procedures cost effectively such that computer security risks are reduced to an acceptable level.

20) E-Government Act of 2002 (Pub. L. 107-347**)**[142]

The purpose of this Act is to …improve the management and promotion of electronic government services and the method by which government information (including information on the Internet) is organized, maintained, and made accessible to the public. It establishes a Federal Chief Information Officer within the Office of Management and Budget, who is charged with establishing this framework.

21) The Sarbanes-Oxley Act of 2002 (Pub. L. 107-204**)**[143]

Part A of this Act establishes rules that publicly reporting enterprises must adhere to concerning the control over their financial reporting systems and assets, including information assets.

[141] For a copy of this Act, please see: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf . In a document released July 22, 2009 by Booz Allen Hamilton and The Partnership for Public Service, it appears the objectives of this Act are not being met. For a copy of the full Booz Allen report please see: http://ourpublicservice.org/OPS/publications/download.php?id=135

[142] For a complete copy of the Act, please see; http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf

[143] For a copy of this Act, please see: http://www.soxlaw.com/

22) The Real ID Act of 2005[144]

This Act has numerous provisions but a leading provision is for uniform information to be placed on States' drivers' licences which is to also be incorporated into a smart chip embedded in the license.[145]

23) Genetic Privacy Bill of 2007[146]

This Bill prohibits the use of genetic information regarding the obtaining of health insurance or employment.

24) FISA Amendments Act of 2008 - Public Law No: 110-261 [147]

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 or FISA Amendments Act of 2008 - Title I: Foreign Intelligence Surveillance - (Sec.

---

[144] For a complete copy of this Act, please see: http://www.ncsl.org/IssuesResearch/Transportation/REALIDActof2005/tabid/13582/Default.aspx . In a report titled "Real ID" in the July 13, 2009 issue of Federal Computer Week (http://www.fcw.com), pp 21-22, it was reported that only five states are complying with this Act, and that 15 have refused to comply, while the remaining states have this issue under legislative review.

[145] Numerous states have protested the requirements of this Act as violating States' Rights. The Department of Homeland Security has countered that if States fail to comply, their citizens may be refused access to air travel. In essence if the states all comply with the requirements of this Act, the U.S. will have a de facto national ID card.

[146] For a complete copy of this Act, please see: http://www.ornl.gov/sci/techresources/Human_Genome/resource/privacy/privacy1.html

[147] This Act is very important because it essentially permits what the Fourth Amendment to the U.S. Constitution prohibits – search and seizure without a warrant. For a copy of the Act please see: http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.06304: Legal Commentator Glenn Greenwald writes; "In *The New York Times* last night, James Risen and Eric Lichtblau -- the reporters who won the Pulitzer Prize for informing the nation in 2005 that the NSA was illegally spying on Americans on the orders of George Bush, a revelation that produced no consequences other than the 2008 Democratic Congress' legalizing most of those activities and retroactively protecting the wrongdoers -- passed on leaked revelations of brand new NSA domestic spying abuses, ones enabled by the 2008 FISA law. The article reports that the spying abuses are "significant and systemic…" For a complete reading of this piece, please see: http://www.salon.com/opinion/greenwald/2009/04/16/nsa/

101) Amends the Foreign Intelligence Surveillance Act of 1978 (FISA) to add a new title concerning additional procedures for acquiring the communications of certain persons outside the United States.

Authorizes the Attorney General (AG) and Director of National Intelligence (DNI) to jointly authorize, for periods up to one year, the targeting (electronic surveillance) of persons located outside the United States in order to acquire foreign intelligence information, under specified limitations, including: (1) prohibiting an acquisition intentionally targeting a person reasonably believed to be outside the United States in order to acquire the communications of a specific person reasonably believed to be inside the United States...

This Act appears to provide a mechanism for circumventing the basic tenets of the Fourth Amendment to the U.S. Constitution (search and seizure) discussed above. Moreover, this act exempts communication carriers and others such as landlords that provide such access to the government for providing such access.

25) E-Verify Act 2008[148]

This Act was established by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRAIRA), P.L. 104-208, signed September 30, 1996, citation: 8 U.S.C. 1324a. It has been amended several times extending its end date.

Essentially this Act requires employers to verify the legal status of workers and applicants for work in the U.S. Here the government has instituted criminal penalties for failure of employers to comply with this Act. In essence, the government has foisted its responsibility regarding immigration on employers via this Act.

[148] For a complete history of this Act, please see: http://www.ncsl.org/?tabid=13127

I. State Statutes

In addition to these federal statutes, the following states have each enacted privacy statutes:[149]

- Arizona
- California
- Florida
- Hawaii
- Illinois
- Louisiana
- Montana
- South Carolina
- Washington

In many of these states, their Acts provide more protection than those afforded by the U.S. Constitution. As Soma indicates,[150]

> The Colorado Court of Appeals recently explained that 'in every case in which our supreme court has recognized a greater protection under the state constitution than that afforded by the federal constitution, it has identified a privacy interest deserving of greater protection that that available under the Fourth Amendment.'

The U.S. approach to privacy as seen above is fragmented and unclear. The purpose of the law is to establish bright lines such that all know what is permitted and what is not. As can be seen, this initial confusion emanates from the U.S. Constitution itself. Without clearly expressing and establishing a definitive right to privacy in federal law, the issue of privacy has in the main been left up to the courts to define and decide. Some would argue this is de facto legislation from the bench. Moreover, we also see numerous federal statutes that in a piecemeal fashion attempt to address various privacy issues in a less

[149] Soma, supra at 3, pp. 172-173.
[150] Soma, supra at 3, page 174. See also *People v. Rossman*, 140 P.3d 172, 176 (Colo. Ct. App. 2006).

than comprehensive integrated manner. And following along this path, we see states enacting privacy laws that are more protective than federal laws. Such a condition begs for clarity and codified guidance on what privacy is, what rights exist relative to privacy, what roles and responsibilities should exist regarding privacy, and what penalties will be enforced for breaches. Perhaps the place for the U.S. to begin such work relative to privacy is to take the EU approach and start with defining in a comprehensive manner data privacy rights.

VI Technology Challenges to Privacy

A. Lay of the Land

The rate of change regarding technology innovations and inventions is absolutely staggering. Just over 100 years ago, the first plane flight was recorded in 1903.[151] At this time, the world was still significantly agriculturally based with a majority of the world's population living in rural or non-capital cities. Yet only some 66 years later in 1969, a man landed on the moon.[152] And as of May 2009, a majority of the world's population lives in major cities.[153]

Like aviation and population shifts, communications tools and infrastructures have likewise undergone significant changes in a relatively short period of time.[154] Here we see the first invention of the computer in 1936, a relatively simple device of limited capability called the Z1. Yet today we see the Criterion Cube Computer, a 20 inch cube

[151] Please see: http://www.wright-house.com/wright-brothers/wrights/1903.html
[152] Please see: http://news.nationalgeographic.com/news/2009/07/090721-apollo-11-moonlanding-facts.html
[153] Please see: http://news.ncsu.edu/releases/2007/may/104.html
[154] Please see http://inventors.about.com/library/blcoindex.htm for a history of the computer.

box that supports 50,000 simultaneous users and requires no special air conditioning or power.[155] Driving much of this technology growth and capability was the shift from vacuum tubes to integrated circuits and from predominantly hardware to software solutions, and from a physical (wired) to an untethered (wireless) world.[156] At the same time via the invention of the voice encoder (vocoder), voice was becoming data via the digitization of the analog voice wave form to a digital form. And as we progressed from breakthrough to breakthrough, data grew and transformed our lives.[157] The vast majority of information was also being created in an unstructured manner (text), versus structured formats (field, record, file format hierarchical structures). Moreover, digital and optical disk technology improved at an exponential rate at the same time permitting vast amounts of data to be amalgamated and retained very economically. As data collections grew, so did the software technologies to search and gather intelligence from the data contained in these digital and optical repositories.[158] And each of these advances became less and less expensive and easier to use making them available to and useable by most. At the same time much of this data was being made available via Internet connections. In July 2009, Forrester estimates the Internet will grow to 2.2 billion users by 2013.[159]

---

[155] For information on the Cube Computer please see: http://www.criterion-sys.com/thecube.php

[156] Verizon Corporation estimates that in the U.S. in 2007, wireless subscribers surpassed wireline subscribers. Please see: http://investor.verizon.com/profile/industry/pdf/industryoverview.pdf

[157] Supra at 22, 25, and 26.

[158] Please see http://lymba.com/company/ This company has developed the most comprehensive software and intelligent bots and spiders that can glean intelligence from vast and apparently unrelated data elements even though these data elements are held in numerous separate repositories. Collectively these tools are known as Natural Language Processing (NLP) tools.

[159] For a copy of the release of the Forrester report, please see: http://news.cnet.com/8301-1023_3-10291796-93.html

Moreover today, our economic wealth is now represented by bits and bytes and military weapons and war fighting strategies are based on a digital theater. In fact, our very beings have become digitized with vast amounts of personal information now collected and stored in commercial repositories. The entities that control these data repositories literally 'sell each of us' via the sale of our digital avatars (digital dossiers).[160] In fact, just this month, The Wall Street Journal reported that Google was improperly, if not illegally, intercepting and collecting vast amounts of personal information from unsecured Wi-Fi nodes across the country.[161]

This change from a hardware driven solution to a software driven one where communications is moving to a more and more untethered environment has afforded the mal intended with a near infinite means to reach others, and essentially enter their private lives from a distance.[162] However, this threat is not limited to the wireless arena as the Internet has essentially connected each of us to the other in a 'One to All' relationship regardless of the communication technology we employ.

---

[160] Please see the following entities as a representative sample of entities that sell vast amounts of private data. ChoicePoint Corporation at http://www.choicepoint.com/, Accurint at http://www.accurint.com/, Experian Corp. at http://www.experian.com/, Transunion Corp. at http://www.transunion.com/ , Equifax Corp. at http://www.equifax.com/home/ , Acxiom Corp. at http://www.acxiom.com

[161] Vascellaro, J. "Google Says It Mistakenly Kept Data On Web Usage," The Wall Street Journal, May 15, 2010, p.B1.

[162] The FBI issued important warnings to those traveling to the China Olympics in 2008 regarding the interception of their communications. Please see: http://www.cbsnews.com/stories/2008/08/07/eveningnews/main4329769.shtml

B. Fundamental Concerns

The ability to create, store, search, cull, disseminate, and make intelligence of vast amounts of data where each is connected to the other, challenges the very premise of all good controls and security: namely; Borders and Trust. By establishing the Internet as such in a 'One to All' connected environment, we have literally extended borders and trust to all in the name of efficiency and effectiveness, often without concern for the threats and risks that devolve. We have mitigated the previous privacy protections of time, distance, and human memory. And by having so much personal information about ourselves being collected and held in commercial and government data repositories, we have literally created a permanent memory concerning our private selves and invited all electronically into our private lives whether we realize the degree to which this intrusion is taking place or not.

As Solove points out,

> …just one firm, Wiland Services maintains a database of about 1,000 different points of information on over 215 million individuals.[163]
>
> Launched in 2003 Regulatory Data Corp. has created a massive database to investigate people opening new bank accounts… This database collects data from over 20,000 different sources around the world.[164]

The economic incentive is just too great to stop this voracious data collection, storage, and dissemination monster. Solove estimates that in 2001, almost a decade ago, the U.S. had direct marketing (database marketing) revenues approximating $2 trillion, and this

[163] Solove, J. 2004. The Digital Person, p. 3.
[164] Supra at 162, p.21.

activity was growing at twice the rate of the U.S. Gross Domestic Product.[165] And Verizon Corporation just reported in its 2009 Data Breach Investigations Report that electronic breaches in the past year exceeded the total number of the previous four years' breaches, exceeding 295 million reports.[166] The financial sector represented 30% of these attacks. Here attackers sought personal financial privacy information.

C. Lack of Effective Controls

Because of the ill defined and diffused legal foundation regarding privacy in the U.S. in particular and the sheer size of private information already in commercial and governmental databases, implementing adequate privacy controls will be most difficult at this late date. As was indicated in the latest Booz Allen study regarding compliance with the requirements enacted under FISMA, entities are not meeting those requirements in material ways.[167] Additionally, by creating such valuable targets where our very persona and economic wealth are maintained in the form of bits and bytes, a situation exists that parallels what Willy Sutton, the famous U.S. bank robber found and stated when asked why he robbed banks, "Because that is where the money is!"[168] Today, the Internet provides many points of access unlike days of old where one only had so many doors and windows in the 'bank' with which to be concerned. However, other such data losses exist. Take for example copier machines. Such modern devises

---

[165] Supra at 162, p. 19.

[166] 2009 Data Breach Investigations Report, April 2009. Verizon Corporation. The report may be viewed at: http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

[167] Supra at 141.

[168] Willy Sutton at http://www.fbi.gov/libref/historic/famcases/sutton/sutton.htm

have hard disks that store in memory some 25,000 to 250,000 data images. Yet when such devices are routinely sold after several years' use, many such machines are sent overseas for resale without the disks ever being scrubbed.[169] A criminal's treasure trove for sure.

As was also seen earlier, many legal scholars propose a definition of privacy as the ability to 'control' information about oneself. However, many commercial enterprises in the U.S. require all kinds of personal data before they will provide services, and their use policies permit them to use, exchange, or sell one's personal information in a manner where personal 'control' is in essence lost. Hence, technology and use policies have made this concept of personal 'control' over our private information moot in the main. This issue is amplified by the cross selling or exchange of so much collected information from one enterprise to another, where each is able to fill in a digital mosaic that becomes our digital dossier.

While the Gramm-Leach-Bliley Act has a requirement that parties be permitted an 'opt out' option regarding the sharing of their private financial information, most fail to exercise this right. This human behavior may be reflective of a similar act where many receiving audit confirmations just trash them and do not respond. Audit confirmation response rates are estimated to only approximate 3%.[170] Conversely, phishers (parties that attempt to have others give up their private information via Internet ploys) are reported to have an estimated 10%

[169] Keteyian, A. "Digital Photocopiers Loaded with Secrets." CBS Interactive, Inc. April 15, 2010. http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shmtl

[170] American Institute of Certified Public Accountants content in Forensics and Financial Fraud course.

response rate - three times better than auditor confirmation rates.[171] So it appears human behavior, commercial incentives, social engineering, and technology exploits often work in concert to defeat the 'control' aspect regarding one's personal information.

The Federal Trade Commission (FTC) in the U.S. estimated that Identity Theft in 2005 affected 8.3 million U.S. parties (just over 3% of the U.S. population in a single year).[172] Moreover, at a Federal Deposit Insurance Corporation (FDIC) conference on ID Theft, it was indicated that the police in most jurisdictions do not even want to take an ID Theft report as they are unsure where the crime took place if carried out over the Internet, and therefore they do not know if they have jurisdiction.[173]

As to existing technology controls for protecting private information, we see breakdowns across the globe. Some of these breakdowns are unintentional, while many are mal intended. Typical examples range from firms losing their clients' data when sending tapes to backup facilities, to major thefts of privacy data such as at TJX in the U.S. and at major food chains in Europe. [174]

---

[171] Symantec estimates this 10% rate. Please see http://www.symantec.com/norton/cybercrime/phishing.jsp

[172] For a copy of the FTC report, please see: http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

[173] In many jurisdictions the local police lack the resources, both financial and in trained personnel, to effectively carry out ID theft investigations. Please see: http://www.fdic.gov/news/conferences/identity_theft/

[174] The following examples are merely representative examples and in no way constitute an inclusive list. Ameritrade, a major brokerage firm, lost client data back-up tapes. Please see: http://www.securityfocus.com/news/11048. Marriott loses customers' data with the loss of backup tapes: http://news.cnet.com/Marriott-loses-data-on-200,000-customers/2100-1029_3-6015768.html. Bank of America loses clients' data via a loss of backup tapes at http://www.csoonline.com/article/220537/No_More_Lost_Backup_Tapes_Chain_of_C

D. New Threats

The advances in technology concomitant with digital the amalgamation of personal data and the ability to reach such data electronically from almost anywhere, all now stored in permanent memory, has wrought tremendous privacy challenges. Compounding this situation of creating a 'target rich environment', technology continues to advance and its rate of increase is surpassing the ability of laws and controls to maintain any form of equilibrium.

In a recent report, it was cited that the amount of malware increased 800 percent in 2007 from the previous year.[175] In another report, some 85% of U.S. organizations realized one or more data breaches between 2008 and 2009.[176] And in March 2008, a security firm announced it discovered a database with over 8,700 stolen FTP server credentials.[177] Moreover, in a recent report it was cited that the U.S. Justice Department declines to prosecute nearly three of every four computer-fraud cases.[178]

---

ustody_Security_Measures. Mal intended attacks: Grocery chains in Europe compromised via wireless exploits embedded in grocery chain credit card readers at http://online.wsj.com/article/SB122366999999723871.html. TJX loses 45 million client records through data theft at http://www.networksystemsdesignline.com/showArticle.jhtml?printableArticle=true&articleId=199500680.

[175] Washkuch, F. 17 January 2008. "Malware up 800 percent in 2007, says Panda," Infosec World. http://www.scmagazineus.com .

[176] "The 2009 Annual Study: U.S. Enterprise Encryption Trends," The Ponemon Institute, July 15, 2009. http://www.net-security.org/secworld.php?id=7760

[177] Vijayan, J. 3 March 2009. "Security Firm Discovers Database with Stolen FTP Server Credentials, " BusinessWeek, p. 9.

[178] Blitstein, R.18 November, 2007. "Online crooks often escape prosecution," Mercury News. http://www.siliconvalley.com/news/ci_7497332?nclick_check=1

Now we see biometric information (fingerprints, eye scans, etc.) being collected and stored digitally. This information is also being stored in Radio Frequency Identity Devices (RFID) such as was seen with Irish passport holders.[179] But there was no shielding of the RFID tags in these Irish passports and their personal information was capturable via RF scanners from significant distances versus the intended few feet.

Massive records of individuals' DNA information are being compiled. For instance, National Geographic has its 'Genographic' Project where it is collecting and cataloguing DNA from people all over the world.[180] Keystroke logging, the capture of all keystrokes of any device connected to a network, has become routine practice by many organizations. Spyware is also seen to be everywhere. Here we saw Sony place spyware in its CD software such that it could spy on its customers, Best Buy sold digital picture frames embedded with malicious code, and Seagate sold hard drives made in Asia which contained hidden malware.[181]

Public place camera surveillance is proliferating. In the City of London for instance it is estimated a person will have his picture taken 300 times in a day.[182] And now a Swedish firm has introduced a

---

[179] Greene, T. 23 October 2006. "Irish Passports go RFID and Naked" The Register. Story may be viewed at: http://www.theregister.co.uk/2006/10/23/smart_chips_for_smart_crooks/

[180] National Geographic Genographic Study https://genographic.nationalgeographic.com/genographic/index.html

[181] Borland, J. 10 November 2005. "Bots for Sony CD Software Spotted Online," ZDNet News. Article may be viewed at: http://news.zdnet.com/2100-1009_22-145559.html

[182] Electronic Privacy Information Center. Article may be viewed at: http://epic.org/privacy/surveillance/

technology to permit the ID'ing of people from their videos, even from videos on the web.[183]

And the threats just continue with the introduction of Global Positioning System devices (GPS) and the ability to track a person by his phone, to the ability to place spyware on Blackberry devices as was reported in the UAE, to the new iPhone encryption being far from hack proof.[184] The volume of additional data now captured via these new technologies and exploits just further works to provide an ability for others to capture private information as well as complete our digital dossiers.

And now we have numerous reports from the U.S. Defense Department that offshore developed software is suspect of having Trojans embedded in it.[185] That is, we are being compromised before we buy a product.

There is quite literally not a day that goes by that some major breach or loss of privacy data is not reported. Hence, in addition to laws and regulations, a better technology solution is needed to protect this private information as we see most parties committing crimes via the computer are not even prosecuted in the U.S.

---

[183] Schenker, J. 24 December, 2007. "Finding faces in the e-Crowd," BusinessWeek, p.70. and Keizer, G. 24 January, 2008. "Best Buy infected digital picture frames," Computerworld, Security Column, article may be viewed at: http://www.compterworld.com

[184] For instructions on how to track a cell phone, please see: http://www.howtodothings.com/electronics/how-to-track-a-cell-phone; Schrek, A. 22 July, 2009. "BlackBerry maker: UAE partner's update was spyware, Associated Press. Foresman, C. 24 July, 2009. "New iPhone hardware encryption not even close to hack proof." Article may be viewed on: http://arsttechnica.com

[185] Hamm, S. and Kopecki, D. 13 November 2006. "The Pentagon: Rethinking the Safety of Software Coded over There," BusinessWeek, p.14.

VII. National Security Issues

National security issues will always trump laws and regulations. This calls back to Maslow's Hierarchy of Needs Model. That is, when people are threatened, behavior often changes. This was seen recently in the U.S. where the FISA Court warrant requirements were circumvented by the Bush Administration after the terrorist attacks of September 11, 2001. The Administration felt the FISA process was an impediment to national security. So we saw the massive warrantless surveillance that ensued. Here too, Europe modified some of its rules regarding airline passenger privacy data exchanges between governments after that same terrorist attack. Hence, governments will carry out their mandates of protecting the homeland from internal as well as external threats. And this mandate will require that governments be capable of reading all communications in order to stop unlawful or harmful activity at its earliest point.

This latter point is evidenced in the number of governments and other entities attacking each other electronically. The Economic Espionage Act cited above requires the U.S. government to report to Congress annually the size and makeup of economic espionage carried out against the U.S.[186] These reports indicate that in the latest ten year period countries attacking the U.S. electronically increased from an estimate of seven nations to over 100 today.

[186] The National Counter Intelligence Executive makes these reports annually. Please see http://www.ncix.gov for the past ten years' reports.

And as was reported in The Wall Street Journal, the U.S. electric grid has been compromised by foreign powers as has one of its largest weapon systems.[187]

Clearly for governments as sovereign states the rule is: "do as I say, not as I do" regarding information privacy where national security is the issue.

VIII. Conclusions and Recommendations

Today, the cat is out of the bag. The U.S. lacks effective controls over privacy data. So much private data is already in the hands of commercial and governmental entities, and the U.S. laws are so diffuse and unclear in certain areas, or completing lacking in others, it will be difficult to now implement in the U.S. comprehensive and effective privacy controls.

Clearly, Europe has taken a much more comprehensive and unified approach to providing privacy regarding its citizens' digital personas in this electronic age. But in Europe as in the rest of the world, we see major mistakes made with vast amounts of privacy information being compromised via lost backup data tapes and disks or lost computers. That is, rules and regulations have not mitigated human frailty.

We also see that those that are mal intended have little fear of capture or prosecution as evidenced by the dramatic increase in the scope and scale of computer crimes and compromises across the globe.

---

[187]Dreazan, Y. and Gorbon, S. May 6, 2009. "U.S. Cyber Infrastructure Vulnerable to Attacks," The Wall Street Journal. Please see http://online.wsj.com/article/SB124153427633287573.html

What is needed is an effective capability to introduce the concept of personal 'control' over one's privacy data.

In the U.S. this process could commence by changing the 'opt out' requirement specified under the GLB Act, to an 'opt in' requirement. This policy change would ameliorate the issue of human behavior identified above.

Next, much as we have with certification authorities today, a requirement could be established that before personal information can be passed from one commercial entity to another, an electronic key must be issued by each party about whom information is to be passed. This key could be appended to the privacy information to be exchanged thereby acknowledging agreement with the data exchange. As this process would clearly slow down commerce, opposition would be great; and would fly in the face of what Siklos states, "Information wants to be free."[188]

Lastly, the entire world needs better information security practices and tools. As a beginning, perhaps information should always be required to remain in an encrypted state except when being read or worked on.

The risks are great, the protections weak, time is short, and these recommendations are only starting discussion points. But we must address with diligence and vigor what Soma calls "birth to death tracking," or we will have a world which many do not want.[189]

---

[188] Siklos, R. July 20, 2009. "No Free Lunch." Fortune Magazine, p. 60.
[189] Supra at 3, p.337.

In sum, privacy in the digital age exists in law and regulation both in Europe and on a fragmented basis in the U.S. However, through one or more; commercial activities, administrative polices, national security interests, human error, or mal intended activities, privacy in practice does not meet the bar of a reasonable expectation ‘to be let alone’.

X. Selected References

Books:

Allen, A. 2007. Privacy Law and Society. Thomson West publishers. ISBN: 978-0-314-16358-5.

Bennett, C. and Raab, C. 2006. The Governance of Privacy. The MIT Press. ISBN: 0-262-52453-8.

Blume, P. 2002. Protection of Information Privacy. DJOF Publishing, Copenhagen. ISBN: 87-574-0497-6.

Chernow, Ron. 2004. Alexander Hamilton. Penguin Books, 2004. ISBN-13: 978-1594200090

Friedman, L. 2007. Guarding Life's Dark Secrets. Stanford University Press. ISBN: 978-0-8047-5739-3.

Helewitz, J. 2004. CyberLaw. Pearson Prentice Hall. ISBN: 0-13-114287-0.

Lessig, L. 2001. The Future of Ideas: The Fate of The Commons in a Connected World. Random House. ISBN: 0-375-50578-4. The author also makes this volume available for free for non-commercial purposes at: http://the-future-of-ideas.com.

Lloyd, I. 1997. Information Technology Law. Butterworths. ISBN: 0-406-89515-5.

Mills, J. 2008. Privacy The Lost Right. The Oxford University Press. ISBN: 978-0-19-536735-5.

Newman, A. 2008. Protectors of Privacy. Cornell University Press. ISBN: 978-0-8014-4549-1.

Rule J. 2007. Privacy in Peril. The Oxford University Press. ISBN: 978-0-19-530783-2.

Solove, D. 2004. The Digital Person. The New York University Press. ISBN: 0-8147-9846-2.

Solove, D. 2008. Understanding Privacy. The Harvard University Press. ISBN: 13-978-0-674-02772-5.

Solove D. and Schwartz, P. 1972. Information Privacy Law, 3rd ed. Wolters Kluwer publishers. ISBN: 978-0-7355-7641-4.

Soma, J. and Rynerson, S. 2008. Privacy Law. Thomson/West Publishing. ISBN: 978-0-314-18134-3.

Westin, A. 1967. Privacy and Freedom. Atheneum. Republished by The Bodley Head Ltd. (April 16, 1970). ISBN-13**:** 978-0370013251.

Journal Articles:

Brown, Jeremy. 2008. "Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places." Berkeley Technology Law Journal, Vol. 23:755, pp. 755-781.

Darrow J. and Lichtenstein, S. 2008. "Do You Really Need My Social Security Number? Data Collection Practices in the Digital Age." North Carolina Journal of Law and technology, Vol. 10, Issue 1, Fall, pp. 1-58.

DeMarco, D. 2006. "Understanding Consumer Information Privacy in the Realm of Internet Commerce: Personhood and Pragmatism, Pop-Tarts and Six-Packs." Texas Law Review, Vol. 84: 1013, pp. 1013 – 1064.

DeVries, W. 2003. "Protecting Privacy in the Digital Age." Berkeley Technology Law Journal, Vol. 18:283, pp. 283- 311.

Doyle, C. and Bagaric M. 2005. "The Right to Privacy: Appealing, but Flawed." International Journal of Human rights, Vol. 9, No.1, pp 3-36, March 2005.

Etzioni, A. 2007. "Are New Technologies the Enemy of Privacy?" Springer Science + Business Media B.V.

Finklea, K. 2009. "Identity Theft: Trends and Issues." Congressional Research Service, 7-5700, R40599, May 27, 2009. www.crs.gov .

Glancy D. 1981. "Getting the Government off the backs of People: The Right of privacy and Freedom of Expression in the opinions of Justice William O. Douglas." Santa Clara Law Review. Vol. 21, pp. 1047-1067.

Glancy, D. 2000. "At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet." Santa Clara Computer and High technology Law Journal, May 2000, pp 1-25.

Glancy, D. 2004. "Privacy on the Open Road." Ohio Northern Law Review. Vol.30, pp 295-351.

Gubins, T. 2008. "Warshak v. United States: The Katz for Electronic Communication." Berkeley Technology Law Journal, Vol. 23:723, pp. 723 -753.

Hoffman, L. and Carreiro, K. "Computer Technology to Balance Accountability and Anonymity in Self-regulatory Privacy Regimes." Paper available at http://www.ntia.doc.gov/reports/privacy/selfreg5.htm

Jones, T. and Peterman, L. "Whither the Family and Family Privacy." Texas Review of Law and Politics. Vol. 4, No. 1, pp. 194-236.

Kerr, O. 2009. "Do We Need a New Fourth Amendment?" Michigan Law Review, Vol. 107:951, pp 951- 966.

Klosek, J. 2005. "Data Privacy and Security Are a Significant Part of the Outsourcing Equation." Intellectual Property & technology Law Journal, Vol. 17, Number 6, June 2005, pp. 15- 18.

Lenow, J. 2007. "First Amendment Protection for the Publication of Private Information." Vanderbilt Law Review, Vol. 60: 1:235, pp. 235-282.

Matchulat, J. 2009. "The Unions Rejoice Act: An Examination of the Intent and Potential Impact of EFCA." Employee Relations Law Journal, Vol. 34, No. 4, Spring 2009, pp. 16-55.

McLaughlin, M. "Global Privacy Law: Legislation, Regulations and Policies Affecting Privacy in the Workplace." Paper presented at the 12th Annual labor & employment Law Conference, May 18-20, Austin, TX.

Paton-Simpson, E. 2000. "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places." 50 University of Toronto Law Journal, pp. 305 – 346.

Poste, G. "Privacy and Confidentiality in the Age of genetic Engineering." Texas Review of Law and Politics. Vol. 4, No. 1, pp. 25-32.

Rackow, S. 2002. "How the USA Patriot Act will Permit Governmental Infringement Upon the Privacy of Americans in the Name of Intelligence Investigations." University of Pennsylvania Law Review, Vol. 150:1651, pp. 1651 – 1696.

Rule, J. 2004. "Toward Strong Privacy Values, Markets, Mechanisms, and Institutions." 54 University of Toronto Law Journal, pp. 183- 225.

Sehgal C. "The Power of the Federal Government in the Electronic Age." Texas Review of Law and Politics, Vol. 4, No. 1.

Smith, K. 1999. "Case Notes: Minnesota v. carter an the Undermining of the Fourth Amendment." Texas Forum on Civil Liberties & Civil Rights, Vol. 4:265, pp. 265- 274.

Solove, D. 2006. "A Taxonomy of Privacy." University of Pennsylvania Law Review 154, pp 477-564.

Soma, J. et al. 2004. "An Analysis of the Use of Bilateral Agreements between Transnational Trading groups: The U.S./EU E-Commerce Privacy Safe Harbor." Texas International Law Journal. Vol. 39 .171, pp 171-215.

Swire, P. 2005. "Introductory Essay for '2004 Privacy Year in Review'." I/S Journal of Law and Policy, Vol.1:2-3, pp. i-x.

Talton, S. 2000. "Mapping the Information Superhighway: Electronic Mail and the Inadvertent Disclosure of Confidential Information." The Review of Litigation, Vol. 20:1, Winter 2000, pp. 271-307.

Thomson, J. 1975. "The Right to Privacy." Philosophy and Public Affairs, Vol.4, No. 4, pp. 295-314.

Vogel, P. 2004. "Cross Border Data Privacy." Paper published and presented at the 17th Annual Computer and Technology Law Institute, May 19-21 2004, Austin, TX.

Westin, A. 2003. "Social and Political Dimensions of Privacy," Journal of Social Issues, Vol. 59, No.2, pp 431-453.

Whitman, J. 2004. "The Two Western Cultures of Privacy: Dignity Versus Liberty." The Yale Law Journal, Vol. 113: 1153, pp. 1153-1221.

Williams, M. 2009. "Privacy Management, The Law and Global Business Strategies: A case for Privacy Driven Design." Innovation and Enterprise Research laboratory, University of Technology, Sydney, Australia, pp. 71-79.

Wimberly, M. 2007. "Rethinking the Substantive Due Process Right: Grounding Privacy in the Fourth Amendment." Vanderbilt Law Review, Vol. 60:1:283, pp 283-323.

Cases Cited:

Ashcroft v. Free Speech Coalition 535 U.S. 234 (2002)

Boyd v. United States, 116 U.S. 616 (1886)

Brandenburg v. Ohio, 395 U.S. 444 (1969)

Briscoe v. Reader's Digest Ass'n., 4 Cal. 3d 529 (Cal. 1971)

Candebat v. Flanagan, 487 So. 2d 207, 209 (Miss 1986)

Carson v. Here's Johnny Portable Toilets, 698 F. 2d 831 (6th Cir. 1983)

Castro v. NYT TV, 370 N.J. Super 282 (N.J. Super. Ct. 2004)

Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975)

Deaton v. Delta Democrat Publishing Co., 325 So. 2d 471, 473 (Miss 1976)

Desnick v. ABC, 44 F3d 1345 (&t Cir. 1995)

Doe v. Bolton, 410 U.S. 179 (1973)

Doe v. Evans, 814 So. 2d 370, 373-75 (Fla. 2002)

Engblom v. Carey, 677 F. 2d 957 (2d Cir. 1982)

Felsher v. University of Evansville, 755 N.E.2d 589 Ind. 2001)

Fowler v. Southern Bell Tel. & Tel. Co., 343 F.2d 150, 156 (5th Cir. 1965)

Griswold v. Connecticut, 384 U.S. 479 (1965)

Kastigar v. United States, 406 U.S. 441 (1972)

Katz v. United States, 389 U.S. 347 (1967)

Kyllo v. United States, 533 U.S. 27 (2001)

Lake v. Wal-Mart Stores, Inc. 582 N.W.2d 231 (Minn. 1998)

Lovgren v. Citizens First Nat'l. Bank, 126 Ill. 2d 411 (Ill.) (1989).

Melvin v. Reid, 112 Cal. App. 285 (Cal. Ct. App. 1931 – Superseded by statute)

Meyer v. Nebraska, 262 U.S. 390

Minnesota v. Carter, 119 S. Ct. 469

Nader v. General Motors Corp., 307 N.Y.S.2d 647 (N.Y. 1970)

New York Times v. Sullivan, 376 U.S. 254, 284-95 (1964)

Olmstead v. United States, 277 U.S. 438 (1928)

Pavesich v. New England Life Insurance Co., 122 Ga. 190, 50 S.E. 68 (Ga. 1905)

Plaxico v. Michael, 735 So. 2d 1036 (Miss. 1999)

Prince v. Massachusetts, 321 U.S. 158 (1944)

Reno v. American Civil Liberties Union, 521 U.S. 844 (1997)

Reynolds v. United States, 98 U.S. 145 (1878)

Sidis v. F-R Pub. Corp, 113 F.2d 806 (2d Cir. 1940)

Stanley v. Georgia, 394 U.S. 557 (1969)

State v. Williams, 158 Wn.2d 904, 148 P.3d 993 (Wash. 2006)

Whalen v. Roe, 429 U.S. 589 (1977)

Wheaton v. Peters, 33 U.S. 591, 634 (1834).