

References

Abril, P. S. (2007). Recasting privacy torts in a spaceless world. *Harvard Journal of Law & Technology*, 21(1), 1-47.

Against the already tangled backdrop of privacy law, the Internet age--with its chat rooms, webcasting, blogs, e-mail, instant messaging, text messaging, camera phones, and OSNs--has further complicated the definition of privacy. New technologies have enabled novel social situations that generate privacy harms and concerns that were unforeseeable. Asks whether the public disclosure tort is applicable and relevant in the face of recent technological developments, such as OSNs (online social networks). Systematically reviews the evolution of the tort, provides an overview of the mechanics of popular OSNs and a description of some of the new privacy concerns they have created. (Excerpted from author).

Alban, D. (2009, September 29). *Will your privacy be compromised online?* - CNN.com. Retrieved September 29, 2009, from <http://www.cnn.com/2009/TECH/09/28/online.security.tactics/index.html>

Highlights how e-mail scams and fraud are working to compromise Internet users privacy and security. Discusses likely reasons behind data breaches in the United States. Outline several tips to keep your information secure while online.

Albrecht, K. (2008, September). RFID tag -- you're it. *Scientific American*, 299, 72-77. An overview of RFID (radio-frequency identification) technology, and the use of RFID tags in everyday items that are a part of our daily lives. What once used to track inventory and supplies can theoretically be used to track people, using the tags they are carrying with them, sometimes unknowingly. Calls for legislators to address the risks to individuals from such a technology.

B., K. (n.d.). *Teen Ink - Opinion - Pop culture/Trends - Sexting: Know the Facts.*

Retrieved September 29, 2009, from http://www.teenink.com/opinion/pop_culture_trends/article/131108/Sexting-Know-the-Facts/

Addresses the popular teen phenomenon of "sexting" -- sending risque photos via text messages on cell phones. Discusses some of the possible/likely consequences that come from eventual misuse of the photos. Opinion article, warning against the dangers of "sexting."

Bartee, A. (2006). *Privacy rights: cases lost and causes won before the Supreme Court.* Lanham, MD: Rowan & Littlefield.

This book presents a study of the judicial process as it confronts four privacy issues: birth control, gay rights, abortion, and the right to die. The moral questions surrounding these subjects create intense and enduring debates about the scope and limits of the right to privacy. In four historic cases the right to privacy was struck down by the Supreme Court; in four later cases these

rulings were overturned. Why? This book explains the original failure by analyzing attorneys' mistakes, miscommunication in the judicial conference, attitudes and policy predilections of the justices, and the negative attitudes of state officials and interest groups. The ultimate win for privacy rights is an exciting story involving well know cases like *Lawrence v. Texas*, *Planned Parenthood v. Casey*, *Griswold v. Connecticut*, and the case of Terri Schiavo. (From Amazon.com). Provides a recent base of privacy rulings as a jumping-off point to examine possible rulings relating to the future of privacy.

- Bennett, J. (2009, May 4). A tragedy that won't fade away. *Newsweek*, 153, 38-40.
The article discusses the case of Christos and Lesli Catsouras. Accident scene photos of the body of their deceased daughter Nikki from a motor vehicle crash on October 31, 2006 were leaked onto the Internet. Outlines the family's efforts to stop the circulation of the pictures, in the larger frame of the difficulties of getting something off the Internet once it has been posted.
- Bradley, T. (2009, September 25). *Protect your privacy on Facebook and Twitter*. Retrieved September 29, 2009, from http://www.computerworld.com/s/article/9138505/Protect_your_privacy_on_Facebook_and_Twitter
Referencing President Obama's speech to students, where he warned about watching what they post online, goes into ways to safeguard your privacy using online social networking tools Facebook and Twitter. Discusses ten tips/issues -- from phishing to knowing who can see what and how to control that.
- Brown, E. (2009, September 21). *MySpace drinkin' photos causing real life problems again : Internet law - Evan Brown - Internet Cases*. Retrieved September 29, 2009, from <http://blog.internetcases.com/2009/09/21/myspace-drinkin-photos-causing-real-life-problems-again/>
Highlights a specific case in Texas -- *Mann v. Department of Family and Protective Services* -- that points to the dangers/powers of social networking sites. Woman had her child taken away after placing photos of her drinking & intoxicated on her MySpace page.
- Brown, P. (2008, September). Privacy in an age of terabytes and terror. *Scientific American*, 299, 46.
This introductory article lays out several of the key issues and questions regarding privacy. Mentioned for further review in articles that follow are: privacy vs. security; government monitoring in the age of terrorism; health care; new technologies that place privacy at risk and means of protecting privacy.
- Chandler, A., Gelman, L., & Radin, M. J. (2008). *Securing privacy in the Internet age*. Stanford, CA: Stanford Law Books.
The Internet Age has created vast and ubiquitous databases of personal

information in universities, corporations, government agencies, and doctors' offices. Every week, stories of databases being compromised appear in the news. Yet, despite the fact that lost laptops and insecure computer servers jeopardize our privacy, privacy and security are typically considered in isolation. Advocates of privacy have sought to protect individuals from snooping corporations, while advocates of security have sought to protect corporations from snooping individuals. This book aims to merge the discussion of these two goals. (From Amazon.com).

Collier, A. (2009, September 24). *NetFamilyNews*. Retrieved September 29, 2009, from <http://www.netfamilynews.org/2009/09/teen-sexting-conviction-upheld.html>

A blog about "kid-tech news for parents," briefly touches on the misdemeanor conviction of Jorge Canal for sexting being upheld. Touches briefly on the history of the case. Highlights the guidelines released by the National Center for Missing and Exploited Children regarding sexting.

Diffie, W., & Landau, S. (2008, September). Brave new world of wiretapping. *Scientific American*, 299, 56-63.

The article addresses the past and future of wiretapping. With the migration of telephone conversations to the Internet, existing laws governing surveillance are coming into question; asking whether or not they are applicable to current and future technologies. Addresses the broadening of surveillance powers that would result from equipping Internet technology for wiretapping of Internet phone calls.

Duke, A. (n.d.). *Topless photo could cost Prejean pageant crown - CNN.com*. Retrieved October 24, 2009, from

<http://www.cnn.com/2009/SHOWBIZ/05/05/california.miss.california/index.html>

Updates the ongoing story (at the time) of Miss California USA Carrie Prejean possibly losing her title because of "breach[ing] her contract" by keeping semi-nude photos a secret. Addresses Prejean's assertion that the photos are an attack against her for her answer during the Miss USA pageant of being against same-sex marriage. Brings the ongoing story up to date, with Prejean's future as Miss California USA in the balance at the time of the article. (She would eventually be stripped of the crown, with pageant officials citing multiple contract breaches aside from the picture controversy).

Dyson, E. (2008, September). Reflections on privacy 2.0. *Scientific American*, 299, 50-55.

The author discusses the issue that several questions of privacy may not be about privacy at all. Matters of security, health policy, insurance, self-presentation are addressed as privacy issue imposters. The author emphasizes clearly defining privacy, separating it from its imposters, before focusing on privacy itself.

Echegaray, C. (2009, September 28). *Doctors mistakenly fax patients' data to Indiana company*. Retrieved September 29, 2009, from www.tennessean.com/article/20090928/NEWS01/909280333/Doctors+mistakenly+fax+patients++data+to+Indiana+company

Discusses a specific case in Tennessee where doctors offices have been sending sensitive patient information to the wrong fax number, creating a huge privacy issue. Touches on it not being the first time something like this has happened and how the state agency knew about the problem for over a year.

Garfinkel, S. L. (2008, September). Information of the world, unite!. *Scientific American*, 299, 82-87.

The concept of data fusion -- linking existing databases together -- is to eventually create a massive information resource that is better than the sum of its parts. Privacy advocates are concerned of the power such an all-in-one database would possess. Issues with differences in formatting, errors and duplicate entries have limited the use of data fusion to a few arenas.

Giffen, M. (2008, March). Online privacy. *Current Health* 2, 34, 8-11.

An article on the topic of teens and their tendency to "overshare" their lives on the Internet. Outlines some safety measures to follow to protect oneself when posting online. Includes a brief interview with Amy Polumbo, former Miss New Jersey, discussing when pictures from her private Facebook account ended up in the press.

Givens, B., & Clearinghouse, P. R. (1997). *Privacy Rights Handbook*. New York: Harper Perennial.

In our technologically advanced world, sensitive information about you--from your medical history to your net worth--can be collected without your knowledge and sold to the highest bidder that information may have been taken from records without your permission, or you may have unwittingly revealed it yourself in the course of a normal day. The good news is that you can fight back.[Author] gives you all the information you need to be aware of threats to your privacy and how to aggressively protect it. Outlines how to stop junk mail and telemarketers, guard your online activities, how to find out what's contained in your medical and credit reports (and how to correct any mistakes), lower your risk for identity theft and use the Freedom of Information Act to your advantage. (In part from Amazon.com).

Interviews are not supported in bibliographies by APA. Notation listed at the end of the bibliography.

Hennigan, W. (2008, June 22). Travelers accept body scanners as 'wave' of future. *The Washington Times*, pp. A01.

Article addresses the use of new millimeter wave scanners at airport security. Privacy advocates insist it amounts to a "virtual strip search" with the danger of the scan images being leaked, further violating individual privacy.

Transportation Security Administration officials are working to educate and rebut privacy concerns.

Humbach, J. (2009, September 9). *SSRN - 'Sexting' and the First Amendment*. Retrieved September 30, 2009, from papers.ssrn.com/sol3/papers.cfm?abstract_id=1470819

"'Sexting' and other teen autopornography are becoming a widespread phenomenon, with perhaps 20% of teenagers admitting to producing nude or semi-nude pictures of themselves and an ever greater proportion, perhaps as many as 50%, having illegally received such pictures from friends and classmates. It is, moreover, beginning to result in criminal prosecutions, and the statutory penalties are severe. Given the reality of changing social practices, mores and technology utilization, today's pornography laws are a trap for unwary teens and operate, in effect, to criminalize a large fraction of America's young people. As such, these laws and prosecutions represent a stark example of the contradictions that can occur when governmental policies and initiatives built on past truths and values collide with new and unanticipated social phenomena. ... the language and reasoning ... of *Ashcroft v. Free Speech Coalition* gives strong reason to believe that the scope of the categorical exclusion for child pornography should be closely aligned with the governmental objectives that Ferber and Osborne relied on - which would mean constitutional protection for teen sexting and autopornography that occur on the teens' own initiative. (Taken in part from abstract).

Improving online security. (2008, September). *Scientific American*, 29, 96-99.

A portion of a round-table discussion involving industry leaders in security, privacy and protection. Common solutions raised are upgraded technology and more attention to the human and legal factors affecting privacy or the lack thereof.

Jain, A. K., & Pankanti, S. (2008, September). Beyond fingerprinting. *Scientific American*, 299, 78-81.

Discusses the use of biometric technology as possibly the best defense against identity theft. Outlines biometric system benefits of being harder to bypass and easier to use than tradition card or password security. Cites higher than acceptable error rates as a barrier to more widespread use of the technology.

Jasper, M. C. (2009). *Privacy and the Internet Your Expectations and Rights Under the Law (Oceana's Legal Almanac; Law for the Layperson)*. New York: Oxford University Press, USA.

The Internet is the most significant medium of both commercial and financial communications and transactions. It has become the nation's primary vehicle for the exchange of news, mail, and general information. [T]hese benefits often expose Internet users to serious privacy risks which may have catastrophic results. Thus, it is crucial that Internet users understand how to safely and securely "surf the net," without exposing themselves to criminal activities

which infringe on their privacy. This almanac discusses some of the most important security methods, including the effective use of passwords, utilizing virus software, installing firewalls, understanding encryption technology, and being vigilant about the type of information one shares on the Internet. Internet identity theft is also addressed. In addition, this fully revised publication outlines Internet privacy policies and applicable laws placed upon various entities designed to protect private information of Internet users. A discussion of online privacy protection for children, which encompasses the governing laws are included. Finally, this almanac sets forth the role of the Federal Trade Commission (FTC) in enforcing privacy rights, including a review of some of the major enforcement cases brought by the FTC. The Appendix provides resource directories, applicable statutes, and other pertinent information and data. The Glossary contains definitions of the terms used throughout the almanac. (From Amazon.com).

Johnson, J. W. (2005). *Griswold V. Connecticut: Birth Control And The Constitutional Right Of Privacy (Landmark Law Cases & American Society)*. Lawrence, Kansas: University Press of Kansas.

Americans value privacy as one of their most cherished rights, yet the word "privacy" isn't even mentioned in the U.S. Constitution. It took the Supreme Court's ruling in *Griswold v. Connecticut* (1965) to bestow constitutional protection upon this right. That remains one of the Court's most hotly debated rulings and led directly to an even more controversial decision in *Roe v. Wade* (1973). Explores *Griswold's* origins in a challenge to Connecticut's 1879 anti-contraception law, provides a detailed narrative of its progress, examines the unfolding of the newly secured right of privacy up to recent controversies over same-sex relations, and grounds the story in two key contexts: the struggle within one state to establish the right to birth control and the national debate over the right of privacy. Offers insights into the Supreme Court decision in *Poe v. Ullman* (1961), which rejected challenges to the Connecticut's law and was itself immediately challenged. Traces the progress of *Griswold's* case and clarifies how privacy or "the right to be let alone" became a judicially constructed right. In one of the most idiosyncratic opinions in the Court's history, Justice William O. Douglas ruled that "emanations" from five constitutional amendments afforded protection to the right of privacy, while several other justices proposed competing rationales in support. (From Amazon.com).

Kang, J., & Buchner, B. (2004). Privacy in Atlantis. *Harvard Journal of Law & Technology*, 18(1), 229-267.

Takes an unusual approach to privacy issues in the face of the rising influence of cyberspace. Examines concerns and questions in a play-like format through the "characters" of the Counselor, Philosopher, Economist, Merchant and Technologist.

Kohlmeier, G. (2007). The risky business of lifestyle genetic testing: protecting against

harmful disclosure of genetic information. *UCLA Journal of Law & Technology*, 11(2), 1-58.

The technological and scientific advances of nutrigenetic testing imply that the future is here, but unfortunately the legal protections are not. Nutrigenetics -- the newly developing science correlating diet and genotypes -- promises an easier way to escape the consequences of unhealthy lifestyles. The enthusiasm for nutrigenetics may obfuscate the unusual problems surrounding protection of genetic information, particularly in a market context. Upon providing genetic material, an individual has little control over who can access the results. The ramifications raise considerable liberty concerns -- from privacy and equal protection to perhaps even property rights issues -- and can result in widespread, irreversible damage, such as stigmatization and discrimination against the tested individual and all who share that genetic material. Current regulations and safeguards inadequately address problems posed even when genetic information is accurate, failing to sufficiently consider who may obtain the information. (From abstract).

Kroepsch, A. (2008, March 31). Good practices, good privacy. *CQ Weekly Online*, 806.

Retrieved August 28, 2009, from

<http://library.cqpress.com/cqweekly/weeklyreport110-000002693902>

On the heels of another missing government laptop (in this instance from the National Institutes of Health) with individual's personal data, points the finger at carelessness and lack of enforcement. Outlines privacy 'good practices' that can be implemented or existing ones be enforced, in addition to the Privacy Act of 1974.

Lysyanskaya, A. (2008, September). How to keep secrets safe. *Scientific American*, 299, 88-95.

Addresses modern cryptography and the current technologies available to help protect one's privacy. Explains the benefits of the technologies, from keeping your identity anonymous, to keeping eavesdroppers out. Frames the technology as possible solutions to the privacy problem.

McCarthy, J. (2009). *The rights of publicity and privacy*. St. Paul, MN: Thomson/West.

This book includes actual text and research references for selected state statutes in addition to covering state common law, and federal and foreign law. Outlines the history and development of the rights of publicity and privacy; policy reasons for the right of publicity; elements of infringement; who and what are protected; a survey of legal rights; legal sources defining rights; Constitutional issues; infringing use of personal identity in a commercial setting and in the media; postmortem right of publicity; assignments and licenses; procedure, remedies, and defenses. (In part from <http://west.thomson.com>).

McCullagh, D. (2003, March 25). *Scanning the future of privacy* - *CNET News*. Retrieved September 29, 2009, from <http://news.cnet.com/2100-1029-994080.html>

Discusses the results of a report released by the National Research Council, suggesting guidelines for authentication technologies. Touches briefly on what that would mean for Internet security and protection of information/privacy. Includes comment from Marc Rotenberg from EPIC.

Moss, E. (2008, July 15). *Future of Media Summit Blog*. Retrieved September 29, 2009, from

http://futureexploration.net/fom/2008/07/future_of_privacy_personalised.html

Discusses the future of privacy & personalized advertising in relation to the collection of personal data from users. Addresses the privacy concerns and possible ways to counteract them. High-level overview of the issue, touching on a few key points.

Nehf, J. P. (2007). Shopping for privacy on the Internet. *Journal of Consumer Affairs*, 41, 351-365.

Privacy is a concern for all major stakeholders in modern society, and technology to erode privacy continually emerges. Studies show that individuals are concerned about database privacy; yet, they seldom make privacy a salient attribute when deciding among competing alternatives. Although privacy policies are present on many Web sites, Web users rarely bother to read them. Author examines reasons behind such behavior, identifying rational reasons why Web users do not shop for privacy and discussing the implications for the expanding market for consumer information. (From abstract).

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41, 100+.

With the technological advancements that make it easier to collect, distribute, store, and manipulate personal information, consumers are concerned their rights to control their information being violated. However, despite the complaints, it appears that consumers freely provide personal data. The authors address the "privacy paradox" or the relationship between individuals' intentions to disclose personal information and their actual personal information disclosure behaviors.

Oshiro, D. (2009, September 20). *Facebook Data Mining: Truth in Association?*.

Retrieved September 29, 2009, from

http://www.readwriteweb.com/archives/facebook_data_mining_truth_in_association.php

Explains the MIT experiment called "Gaydar" that uses information listed by one's Facebook friends to identify user information. Highlights that such kinds of data mining is possible via Facebook. Questions what the implications are to privacy and security.

Rainie, L., & Anderson, J. (2008, December 14). *The Future of the Internet III | Pew*

Internet & American Life Project. Retrieved September 19, 2009, from <http://www.pewinternet.org/Reports/2008/The-Future-of-the-Internet-III.aspx>
People openly share more intimate details of their lives online every day, and they are flocking to social networks and uploading and/or viewing homemade videos by the millions. Ubiquitous computing is diffusing into everyday life. Much of what goes on in daily life is more visible -- "more transparent" -- and personal data of every variety is being put on display, tracked, tagged, and added to databases. Examines responses to the prediction -- Transparency heightens individual integrity and forgiveness. In 2020, people are even more open to sharing personal information, opinions, and emotions than they are now. The public's notion of privacy has changed. People are generally comfortable exchanging the benefits of anonymity for the benefits they perceive in the data being shared by other people and organizations. As people's lives have become more transparent, an indiscretion in a YouTube video or other pervasive-media form no longer does as much damage as it did back in the first decade of the 21st Century. Carefully investigated reputation corrections and clarifications are a popular daily feature of major media outlets' online sites. (From authors).

Rees, K. (2007, March 14). *Just Another Katie Fan*. Retrieved October 25, 2009, from <http://katiereesblog.com/>
Fan blog about Katie Rees, former Miss Nevada. Post in question was written by Rees herself, explaining the photo controversy that ultimately led to her losing her title.

Ridley, M. (2009, September 24). *Open Content*. Retrieved September 29, 2009, from http://theontarion.ca/viewarticle.php?id_pag=2587
Highlights the growing trend of being able to know more and more about someone based on the information available about them online. Addresses the permanency of digital information. Discusses some recent news items concerning questions of privacy and technology.

Rosen, J. (2000). *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House.
Explores the legal, technological, and cultural changes that have undermined our ability to control how much personal information about ourselves is communicated to others, and proposes ways of reconstructing some of the zones of privacy that law and technology have been allowed to invade. In the eighteenth century, when the Bill of Rights was drafted, the spectacle of state agents breaking into a citizen's home and rummaging through his or her private diaries was considered the paradigm case of an unconstitutional search and seizure. But during the impeachment of President Bill Clinton, prosecutors were able to subpoena Monica Lewinsky's bookstore receipts and to retrieve unsent love letters from her home computer. And the sense of violation that Monica Lewinsky experienced is not unique. In a world in which everything that Americans read, write, and buy can be recorded and monitored in

cyberspace, there is a growing danger that intimate personal information originally disclosed only to our friends and colleagues may be exposed to--and misinterpreted by--a less understanding audience of strangers. Also examines the expansion of sexual-harassment law that has given employers an incentive to monitor our e-mail, Internet browsing habits, and office romances. And he suggests that some forms of offensive speech in the workplace--including the indignities allegedly suffered by Paula Jones and Anita Hill--are better conceived of as invasions of privacy than as examples of sex discrimination. (From Randomhouse.com).

Rotenberg, M. (2009, September 25). *Marc Rotenberg: What's Privacy in the Age of Facebook?*. Retrieved September 29, 2009, from http://www.huffingtonpost.com/marc-rotenberg/whats-privacy-in-the-age_b_299466.html

Elaborates on the growing privacy issues in regards to the increasing use of technology and services like online social networks. Highlights how the changing social rules necessitate a reconsidering of the definition of privacy. Argues that privacy is still a concern and issue, even in the age of hyper-online sharing and Facebook.

Rothstein, M. A. (2008, September). Keeping your genes private. *Scientific American*, 299, 64-69.

The author discusses the current trend of digitizing medical records and genetic testing. With individual's personal medical histories, including genetic profiles, going digital, the question of how to protect that sensitive information from misuse is being raised. Calls for tougher legislation, citing current laws as offering weak protection.

Interviews are not supported in bibliographies by APA. Notation listed at the end of the bibliography.

Simmons, C. (2007). Protecting children while silencing them: the children's online privacy protection act and children's free speech rights. *Communication Law and Policy*, 12(2), 119-142.

In 1998 the U.S. Congress passed the first and only law protecting the privacy of individuals on the Internet. The Children's Online Privacy Protection Act (COPPA) restricts the online collection of personally identifiable information from children under the age of 13. According to COPPA's Final Rule issued by the Federal Trade Commission (FTC) web sites that maintain chat rooms directed at children must either a) condition a child's participation on the prior consent of the child's parent or b) monitor the chat room and censor any references to personally identifiable information. Examines whether COPPA's chat room restrictions infringe on the free speech rights of children under the age of 13. (Excerpted from EBSCOhost abstract).

Interviews are not supported in bibliographies by APA. Notation listed at the end of the

bibliography.

- Solove, D. J. (2008, September). The end of privacy?. *Scientific American*, 299, 100-106. The article tackles the prickly issue of social networking sites and the culture of sharing everything with everyone. Raises concerns that previous definitions and protections of privacy aren't equipped to handle the new technologies and social norms. Calls for existing law to be adapted to offer privacy protection for actions in what used to be considered public.
- Tessler, J. (2006, February 20). Privacy erosion: a 'net' loss. *CQ Weekly Online*, 480-485. Retrieved August 28, 2009, from <http://library.cqpress.com/cqweekly/weeklyreport109-00000205288>
Discusses the growing trend of individuals placing virtually everything online, moving much of their lives to the Internet. With that migration comes lack of protection by current privacy laws. Addresses briefly the gray areas of privacy vs. national security/safety and the government's role in that battle.
- Vijayan, J. (2009, September 22). *Privacy advocates hail Facebook's plan to shutter Beacon*. Retrieved September 29, 2009, from http://www.computerworld.com/s/article/9138373/Privacy_advocates_hail_Facebook_s_plan_to_shutter_Beacon
Article reports the trumpeting of the demise of Facebook's Beacon service, attacked from the outset for its privacy problems. Highlights the major privacy problems with the service that lead to it being shut down.
- Waldo, J., Lin, H., & Millett, L. (2007). *Engaging privacy and information technology in a digital age*. Washington, DC: National Academies Press.
This book presents an examination of privacy in the information age. It explores such important concepts as how the threats to privacy evolving, how can privacy be protected and how society can balance the interests of individuals, businesses and government in ways that promote privacy reasonably and effectively? It also seeks to raise awareness of the web of connectedness among the actions one takes and the privacy policies that are enacted, and provides a variety of tools and concepts with which debates over privacy can be more fruitfully engaged. The book focuses on three major components affecting notions, perceptions, and expectations of privacy: technological change, societal shifts, and circumstantial discontinuities. (From The National Academies Press <http://www.nap.edu>).
- Whitney, L. (2009, September 24). *Survey: Half of businesses don't secure personal data | Security - CNET News*. Retrieved September 29, 2009, from http://news.cnet.com/8301-1009_3-10360639-83.html
Discusses the results of a survey of more than 500 companies by Imperva and Ponemon Institute. Touches on reasons why businesses aren't securing data, not getting up to PCI DSS (Payment Card Industry Data Security Standard) compliance

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: a risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, 49, 86+.

The author examines the different attitudes toward privacy teens often have from adults. Seeks to outline key points of difference between adults and teens and protection needs those differences require.

Interviews

*although interviews are typically not listed in APA bibliographies (only as in-text citations), they're included here for the sake of record

Gaylord, Scott W. Interview. December 3, 2009.

Scott Gaylord is an Associate Professor of Law at the Elon University School of Law in Greensboro, NC. Gaylord teaches constitutional law courses at the school.

Givens, Beth. Radio interview from KUCI-Privacy Piracy. October 12, 2009.

Beth Givens is the founder and director of the Privacy Rights Clearinghouse. The PRC is a non-profit advocacy, research and consumer education program founded in 1992 in San Diego, CA.

Schneier, Bruce. Interview. Email. September 30, 2009.

Bruce Schneier is an internationally renowned security technologist and author. Described by *The Economist* as a "security guru," he is best known as a refreshingly candid and lucid security critic and commentator. Schneier is the Chief Security Technology Officer of BT. (From <http://www.schneier.com/>).

Smith, Robert Ellis. Interview. Email. October 8, 2009.

Publisher of The Privacy Journal, <http://www.privacyjournal.net/>. Frequently used as an expert witness on privacy.p