Advances in Business Research
2012, Vol. 3, No. 1, 43-52

Legal and Ethical Implications of Newspaper Web Privacy Policies

Gundars Kaupins, Boise State University
Christy Suciu, Boise State University
Mark Buchanan, Boise State University

This study summarizes the legal and ethical implications of the privacy policies of the top ten newspapers in the United States. The papers have created policies using language that is more complicated than a typical reader would read. They have allowed themselves to collect data from a wide variety of sources and send the information to third parties can use the information for a variety of purposes. These policies exist in the context of the Fourth Amendment, Electronic Monitoring Communications Act, Wiretap Statutes, and other laws and court cases.

This study analyses privacy policies of the top ten newspapers in the context of massive data collection efforts by the newspapers about their readers. For example, registration requires readers to supply certain personally identifiable information (PII) including e-mail, zip code, age, sex, household income, job and industry to register on the website. Purchases may require name, address, phone, e-mail, credit card number, and other billing information. Third parties who perform tasks required to complete purchase transactions may be needed. Some examples would be fulfilling orders and processing credit card claims (McKenzie, 2009).

User generated content and public activity includes comments, blogs, discussion forums, social networking areas, or other community postings. Any personally identifiable information submitted can be read, collected and used by other users in this area. The networks help newspapers collect stories, keep readers interested in the paper, and connect with other readers. The newspaper assumes no responsibility to publish, take down, remove, or edit any readers' activities.

With contests, sweepstakes and special offers, the newspapers collect information from readers in terms of these optional activities. If any information is shared with third parties, the papers may or may not notify the reader. If the reader does not want to share personal identifiable information, the reader may decline to join, but may lose rights to see various pages.

The newspapers may collect information in connection with voluntary reader surveys, panels, and market research. Data may be collected on websites, the phone or through the mail.

The papers may send text messages upon readers' request through text messaging services. The newspapers can use the information to track access to websites and mobile applications.

All of these methods of interaction allow newspapers to record PII about the readers through a wide variety of methods. Cookies recognize readers and help the paper understand where they are going and how much time they spend there. Analytic technologies help the paper provide information about browsing patterns of readers for marketing and information flow purposes. IP addresses log the location of readers' computers on the Internet for systems administration.

Inappropriate data such as reader location based on photographs can be obtained. When a reader completes a transaction with a third party such as a company that advertises with the newspaper, that third party can provide detailed information about the reader to the newspaper. Third parties can use credit card data obtained from newspapers for various unauthorized purposes.

Crime on the Internet is a continuing problem. For example, in 2011, the Internet Crime Complaint Center (2011) found that for three years in a row it received over 300,000 complaints about Internet transactions, a 3.4-percent increase over the previous year. The adjusted dollar loss of these complaints was $485.3 million.

Purpose

With the many ways to interact with online newspaper readers, serious questions emerge concerning privacy protection of readers. This study summarizes the legal and ethical implications of privacy policies focusing on the privacy policies of the top ten newspaper websites in the United States. Current research literature does not address the comparison of privacy policies in any significant way.

Privacy Comparison Research

Existing research comparing privacy policies of various organizations has been slim. According to Coldewey (2012), a 2011 study of the top 100 U. S. websites as ranked by Alexa in September in 2011 found that 97% of the

sites had a privacy policy. Only 2% of sites had a mobile-optimized privacy policy. For example, user location data may not be protected when the user is on a cell phone when looking at a mobile website. Only 7% of sites showed how long they store user data (and presumably what data is stored), and 32% explained how users can forever delete account data from the website. Much of the information might be available upon request. About 31% of privacy policies stated they share user data with third parties for commercial purposes, 36% collected user location data, and 72% allowed third parties to track users on their site. The average privacy policy was 2464 words long and took about ten minutes to read. The average privacy policy reading level was college sophomore whereas the average American reading level was the 8th grade.

A study by Kaupins and Reed (2012) compared the privacy policies of the top twelve newspaper sites in Latvia, Lithuania, and Estonia. They found that Estonian newspaper websites had the largest number of privacy protections that included limits to reader speech, a disclaimer of responsibility of reader-provided content, policies related to the privacy of personal information received, and the right to edit reader-provided content. There were few privacy protections.

A comparison of five social networking apps indicate that privacy is not protected as well as discussed in their privacy policies though the privacy policies might state that cookies and individual IP addresses are used for internal purposes. However, users' data may be used for third parties to help advertise products across each of the privacy policies (Privacycast.com, 2012).

Legal Research

The United States Constitution, Federal laws, and major court cases combine to provide limited guidance for organizations as they seek to develop privacy policies associated with their websites (Marcus, et. al., 2007). The Supreme Court has found a basis for a constitutional right to privacy in the 1st, 3rd, 4th, 9th and 14th amendments. While the Constitution applies only to government action, its principles often form the basis for legislation that does bind private parties, including business entities such as the top ten newspapers in the United States.

The Fourth Amendment to the Constitution states that people have the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." According to Harlan (2012), the 18th century framers of the Constitution did not have the complications of the Internet in mind. Related to a 4th amendment case involving a secret attachment of a GPS device to a drug dealer's vehicle, Justice Sonia Sotomayor wrote in dicta, "[m]ore fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks" (United States v. Jones, 2012: 19). Note, again, that Constitutional constraints only apply directly to government activity and that statutory enactments are necessary to bind private conduct. However, expectations that arise from constitutionally protected rights can easily lead to greater expectations in the private sphere that can in turn affect the development of new public policy. Gatherers, storers, and users of personally identifiable information need to be aware of growing expectations of privacy and that failure to take measures to address those expectations can and likely will lead to expanded legal constraints. Justice Sotomayor's comments relate to this very point.

The legal landscape of privacy rights that apply to newspapers is still relatively undeveloped. Relevant federal statues associated with the right to privacy include the Children's Online Privacy Protection Act (COPPA) (1998), the Electronic Communications Privacy Act (ECPA) (1986), the Computer Fraud and Abuse Act and the CAN_SPAM Act (2003). The ECPA also encompasses the Stored Communications Act (1986) and the Wiretap Act (1986).

With the Children's Online Privacy Protection Act (COPPA) (1998), websites need verifiable parental consent before collecting personal information about children under 13. Much of the act is extremely relevant to newspaper websites as the potential information collected from children could include e-mail, accounts, chats, bulletin boards, and new media in general. Newspapers and other organizations are required to have their websites post notices of online data collection to kids and parents and allow parents to review personal information collected about children.

The ECPA restricts access to selected computerized records without the consent of the customer. The Stored Communications Act, Title II of the ECPA, restricts the voluntary or knowing disclosure to any person of the content of electronic communications (such as emails) by providers of electronic communications services or remote computing services to the public. It also provides for criminal liability for persons who intentionally access without permission a facility through which an electronic communication service is provided; or intentionally exceeds the permission to access that facility. The Wiretap Act, Title I of the ECPA, provides for civil and criminal liability for any person who intentionally intercepts, uses or discloses the contents of electronic communications. The

interception must be during transmission, as opposed to while in storage (Konop v. Hawaiian Airlines, 9th Cir. 2002), and certain exceptions, such as consent by a party (either the originator or any addressee) to the communication, apply. In Konop, the airlines accessed the plaintiff's website by posing as other pilots, with their consent. However, as those pilots had not yet registered on the site, they were not users and therefore could not give consent to the airlines, rendering its access unauthorized. The ECPA would not apply to interception by or disclosure to any governmental agency that has acquired the appropriate warrant. In re Toys 'R' Us, Inc., Privacy Litig. (N.D. Cal. 2001), the court held the Wiretap Act does not provide a cause of action against mere aiders and abetters.

The Computer Fraud and Abuse Act (1986) provides a cause of action against one who, "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer". Criminal penalties are provided as well as civil actions for compensatory damages and injunctive relief. The term protected computer extends to the full jurisdiction of the federal government and includes that which is used in or affecting interstate or foreign commerce or communication. Access to the computer must be obtained knowingly and with intent to defraud, without authorization with the result of obtaining anything of value worth more than $5,000 in any 1-year period.

Interestingly, a couple of cases have indicated that providers may resolve some issues with an appropriate web site privacy policy and disclosure. In EF Cultural Travel BV v. Zefer Corp. (1st Cir. 2003), the court stated that "lack of authorization [setting up potential liability under the CFAA] could be established by an explicit statement on the website restricting access" to certain portions of information. In Supnick v. Amazon.com, Inc., (W.D. Wash. 2000), Alexa collected the surfing habits of customers and relayed that information to third parties such as Amazon. Under the terms of a court approved settlement agreement, Alexa was required to add privacy policy information to its Web site and implement a feature requiring customers to opt-in to having their personal data collected before they could download Alexa software.

The CAN_SPAM Act (2003) governs commercial electronic mail messages. Such messages must clearly and conspicuously identify the message as an advertisement or solicitation and provide a valid physical postal address of the sender. They must also include a functioning return electronic mail address or other Internet-based mechanism and contain a clear and conspicuous notice of the opportunity to decline to receive further commercial electronic mail messages from the sender. It is unlawful for any person (company) to sell, lease, exchange or otherwise transfer a person's email address for commercial purposes after that person has made a request not to receive some or all messages from the sending company.

The Gramm-Leach-Bliley Act (1999) requires financial institutions to provide their customers with a privacy notice at the time the consumer relationship is established and annually thereafter. The notice must include the customer's right to opt out of any information sharing with unaffiliated parties pursuant to the provisions of the Fair Credit Reporting Act. Such institutions must also have reasonable policies and procedures in place to ensure the security and confidentiality of customer information. These financial institutions may be third parties to newspapers.

The Equal Employment Opportunity Act (1972) restricts the collection and use of information associated with gender, religion, national origin, race, and color that could result in employment discrimination. Discriminatory use of newspaper information may be prohibited.

State laws may also create privacy rights that apply to newspapers. Under the California "Shine The Light" law (2003), customers who are California residents are allowed to request companies, whether located in California or not, to disclose the companies (names and addresses) with which they have shared the individual's personal information for marketing purposes within the last twelve months as well as the nature of the personal information shared. Companies are allowed to preclude such requests by providing customers with notice of their privacy policies containing opt-in or opt-out options. California "Shine the Light" would be explicitly mentioned.

There appear to be common themes among the laws and court cases related to privacy policies. Related to newspaper websites, major actions either prohibited or questionable include:

1. Disclosure of personal data without permission.
2. Collection of selected personal information such as gender, race, religion, national origin and color for certain purposes.
3. Disclosure of financial (public and nonpublic) records for certain purposes.
4. Disclosure of electronic funds transfers for certain purposes.
5. Disclosure of customer information for certain purposes.
6. Unannounced monitoring.

Also, related to newspaper websites, some common actions that are allowed and sometimes required include the following:

1. Development of privacy policies.
2. Compliance with warrants or subpoenas for data.
3. Providing the right to challenge the accuracy of the data.
4. Training record keepers as to sufficient safeguards.
5. Use of data only for business-related purposes.
6. Monitoring disclosures.
7. Disclosure to customers about the use of personal data.
8. Protection of children's data.
9. Prevention of children from entering data.

Finally, even where not constrained by law, newspapers need to be aware of the expectations of their customers, just as with any stakeholders, and address legitimate interests.

Ethics Research

New media such as forums, social networks, blogs, and alerts allow newspapers to share information to the public and have the public share information to the newspapers. To do so, privacy and freedom of speech have to be balanced. Privacy policies are part of the effort to create this balance through appropriate surveillance of what is going on online.

Various Internet surveillance tools are useful for organizations to help protect them against inappropriate blogs, forums, and other ways website users can submit information. Inappropriate communication might involve lies about individuals, discrimination against groups, and other illegal activities (Kidwell and Sprague, 2009; Riedy and Wen, 2010). Surveillance also can help Internet services research customers and thereby create a more efficient design of the website to meet customer preferences and needs (Gage, 2008; Riedy and Wen, 2010).

Unfortunately, surveillance can lead to people discovering significant amounts of information about others that may be inappropriate. Pictures posted to a newspaper showing others in compromising positions that are published on a newspaper site can lead to legal difficulties for the victim, perpetrator and the paper (Timm and Duven, 2008; Hodge, 2006; Duboff, 2007). Personal information may come out that unfairly damages reputations of employees. Sensitive financial and strategic corporate information may be divulged by anyone (Buckley, 2010). Sometimes individuals voice false opinions to foster fallacies within newspaper blogs. Sometimes newspaper users get stalked by anonymous readers of their blog postings. Sometimes online shopping websites connected to newspapers are doubted because a clerk working for that website uses credit card information in an unauthorized way (Buzzle.com, 2012).

According to Reidy and Wen (2010), the surveillance policies within privacy policies must be consistently applied and enforced with secure recordkeeping. Methods should be developed for determining how the data obtained from surveillance is going to be analyzed and how and by whom an appropriate response is determined and implemented. Ultimately, the privacy policies must protect privacy, insure accuracy, protect data and property, and still maintain access of various content providers and readers (Parrish, 2010; Mason, 1986).

Methodology

Newspaper websites in the United States were used in the comparison of websites. One reason newspapers were used was because there is clear data concerning the rankings of various newspapers from 4imn.com (2012). The original aim of 4imn's ranking of newspapers is to promote web publication and electronic access to national and world information. The rankings use web indicators to compare newspaper sites. Newspapers are sorted by the 4imn web ranking. The ranking is based upon an algorithm including three unbiased and independent web metrics extracted from three search engines: Google Page Rank, Yahoo Inbound Links, and Alexa Traffic Rank. The aim of 4imn is to provide a popularity ranking of worldwide newspaper websites. Based on 4imn rankings, the top ten newspaper websites in the United States were chosen for web search comparisons. The privacy policy sites in the top ten list (in order from most popular) include New York Times (2011), Wall Street Journal (2011), Washington Post (2011), USA Today (2011), Los Angeles Times (2011), Examiner (2010), New York Daily News (2012), Chicago Tribune (2011), New York Post (2011), and Philadelphia Inquirer (2007).

One way of measuring whether a privacy policy is legal and ethical is to measure its readability. Difficult words may protect the newspapers because readers may be less inclined to sue the papers if they don't understand the

newspaper privacy policies. The privacy policies are first compared based on reading ease through a variety of measures. According to TRUSTe (2012), privacy policy reading level might be a proxy for policy clarity even though the relationship is not perfect. Measures of reading level include the following:

1. Flesch-Kincaid Reading Ease is a formula that is a function of total words, syllables and sentences that roughly leads to scores from 0 to 100. The lower the score the harder the reading material. About 0-30 is for university graduates, 60-70 is for 13-15 year olds and 90-100 is for 11 year olds (Kincaid, et. al., 1975).
2. Flesch-Kincaid Grade Level is a formula that translates the Flesch-Kincaid Reading Ease formula into approximate grade levels. A score of 9 would indicate that the reading would be understood by a student in the 9th grade. (Reliabilityformulas.com, 2012).
3. Gunning-Fog Score is a function of complex words (three syllabus or more), words, and sentences. A score of 12 translates to a reading for a high school senior (Gunning, 1952).
4. Coleman-Liau Index is a function of the average number of letters per 100 words and the average number of sentences per 100 words. A fourteen would be equivalent to a college sophomore reading level (Coleman and Liau, 1975).
5. SMOG Index is a function of the number of sentences and number of words with three or more syllables. It leads to a grade level of reading (Hedman, 2008).
6. Automated Readability Index is a function of characters (number of letters, numbers, and punctuation marks), words (number of spaces), and the number of sentences. All lead to approximate reading grade levels (Senter and Smith, 1967).
7. Average Grade Level averages the grades of the Flesch-Kincaid Grade Level, Gunning-Fog Score, Coleman-Liau Index, SMOG Index, and Automated Reliability Index.

Another way to compare privacy policies is to analyze how data is collected from readers. Through a content analysis of the privacy policies the authors found which newspapers collected personally identifiable information and non-personally identifiable information through a variety of sources such as blogs, chats, forums, letters to the editor, and e-mails.

In a manner similar to TRUSTe (2012), the authors compare how privacy policies claim to use reader data. Do third parties receive the data? Does the newspaper use the data to provide services requested, statistical analysis, a customizing experience, and e-mail newsletters? How long is the data stored? Can the reader opt out of having data stored?

Results

Results from Table 1 compare the readability scores of the various online newspapers. Even though the New York Times privacy policy has almost doubled the number of words as the other nine online newspapers, its readability was significantly the easiest among the group. The average grade level (11.2) places the privacy policy reading level at the high school junior level. The next lowest paper was the Philadelphia Inquirer with a 12.1 average grade level (high school senior). The highest average score was 15.1 which places the Los Angeles Times (2011) and Chicago Tribune (2011) privacy policy reading levels at the college junior level.

Table 1: Comparison of Privacy Policy Readability Characteristics

Privacy Policy Readability Characteristics	NY Times	WS Journal	Wash. Post	USA Today	LA Times	SF Examiner	NY Daily News	Chicago Tribune	NY Post	Phil. Inquirer
Number of Words	5103	4188	2147	2354	2225	1992	2680	2225	2326	2372
Flesch-Kinkaid Reading Ease	53.6	43.6	40.9	36.3	36.7	36.9	45.4	36.7	43.2	43.0
Grade Level Indices										
1. Flesch-Kinkaid Grade Level	10.4	11.7	11.4	14.9	14.8	13.9	11.9	14.8	12.1	11.3
2. Gunning-Fog Score	12.5	13.3	14.5	17.3	17.3	15.1	14.0	17.3	14.0	13.2
3. Coleman-Lian Index	12.8	14.7	14.5	13.7	14.3	14.0	13.4	14.3	14.1	14.3
4. SMOG Index	9.8	11.1	10.7	13.1	12.9	13.1	10.9	12.9	11.4	10.7
5. Annotated Readability Index	10.6	12.1	10.6	15.6	16.1	14.0	11.9	16.1	12.3	10.8
Average Grade Level (Indices 1-5 averaged)	11.2	12.6	12.3	14.9	15.1	14.0	12.4	15.1	12.8	12.1

Table 2 shows results of a comparison of privacy policy information collection claims. The first part of the table reveals sources of user information in which the newspapers can receive personally identifiable information (PII). All newspapers indicate they can receive PII from billing and credit cards, and third party advertisers. Though all of the newspapers are associated with social networks, only half of them mention social networks in their privacy policies. Blogs, messages, chats, bulletin boards, posts, contest, and sweepstakes are mentioned by a majority of the websites whereas surveys, voting, and polling are mentioned by a minority.

The second part of the table features non-personally identifiable information the newspapers claim they receive from various sources. All of the websites affirm that they use cookies to track reader preferences and IP addresses to report reader information to its various advertisers. Half of the websites affirmed that they could use Global Position System (GPS) data to monitor customer location for those who use mobile devices. Chicago Tribune (2012) affirms that location monitoring is used to target ads that are associated with the location of the reader.

Table 2: Comparison of Privacy Policy Information Collection Claims

Sources of User Information Collected	NY Times	WS Journal	Wash. Post	USA Today	LA Times	SF Examiner	NY Daily News	Chicago Tribune	NY Post	Phil. Inquirer
Personally Identifiable Information (PII)										
Registration	x	x	x	x	x		x	x	x	x
Credit card	x	x	x	x	x	x	x	x	x	x
Social networks	x	x		x	x			x		
Blogs, chats, bulletin boards, posts	x	x	x	x	x	x			x	x
Contests/Sweepstakes	x	x	x		x	x	x	x	x	
Surveys/Voting/Polling	x				x			x	x	
Third Parties (advertisers)	x	x	x	x	x	x	x	x	x	x
NonPersonally Identifiable Information (nonPII)										
Cookies	x	x	x	x	x	x	x	x	x	x
IP Addresses	x	x	x	x	x	x	x	x	x	x
GPS data	x					x		x	x	

Table 3: Comparison of Privacy Policy Information Use Claims

Reader Data Use	NY Times	WS Journal	Wash. Post	USA Today	LA Times	Examiner	NY Daily News	Chicago Tribune	NY Post	Phil. Inquirer
Respond to customer inquiries	x	x	x	x	x	x	x	x	x	x
Send news alerts			x		x			x		x
Notify about new features	x	x	x					x	x	
Administer sweepstakes and contests			x		x		x	x		
Contact customers about interesting content		x	x		x			x	x	
Analyze the accuracy, effectiveness, usability, and popularity of the web pages	x	x	x	x	x	x	x	x		x
Target web pages and advertising	x	x	x	x	x			x		x
Protect the legal rights of the newspaper and its users		x							x	
Share User data with 3rd parties for commercial purposes with notice	x	x	x	x	x	x	x	x	x	x
Disclose how long data is stored										
Incorporate the California “Shine the Light” Law	x	x		x	x		x	x		
Incorporate the Children’s Online Privacy Protection Act	x		x	x		x	x		x	x
Do not guarantee the security of the data received from users	x	x	x	x	x	x	x	x		
Explain how to delete user accounts	x	x	x	x			x			

Table 3 shows a comparison of privacy policy information use claims. All papers process and respond to customer inquiries of questions or services requested. They also share user data with third parties for commercial purposes with notice. However, they are inconsistent in reporting various other uses of reader information. The majority mention analyzing the accuracy and effectiveness of their web pages, compliance with the California ‘Shine the Light Law”, compliance with the Children’s Online Privacy Protection Act, disclaimers of any guarantee of the security of data received from users, and customizing the content of the web for the customer. Half mention notifying readers about new features of their services and contacting readers about information the paper believes

would be of interest. The minority mention sending news alerts, completing a merger or sale of assets of the paper, and protecting the legal rights of the newspaper and its users. No paper disclosed how long the data about readers is secured. Only half explain how to opt out and almost none explain how long they keep customer data.

Discussion

As anticipated, the privacy policies of the top ten online newspapers reveal that the reading level is much higher than the 8th grade level. The New York Times clearly came out best on the readability measures in spite of the fact that the length is twice of other policies. Whether this is intentional or not, newspapers might be able to protect themselves with more difficult language by reducing the chance that readers might sue because they do not understand what is in privacy policies.

Readability can be significantly improved by reducing complicated, byzantine, obfuscated, and convoluted discussions and increasing the use of short words. This does not happen in the privacy policies as shown by the very high grade levels of especially the Chicago Tribune (15.1), Los Angeles Times (15.1), and USA Today (14.9). Their reading levels hover around the college junior level. As an example of the difficulty of reading privacy policies, the following example is classic. This prose is extremely difficult to read that makes understanding the right to share user information challenging.

"We reserve the right to share this information with other Tribune Company business units and affiliates, including for example their affiliated Web sites, and with any entities which Tribune Company subsidiary (collectively, "Affiliates") with agents who may provide services or communicate with you on our behalf; and with third party advertisers and/or contractors with which Chicagotribune.com or an affiliate have a relationship. This policy does not apply to any Affiliate's, third-party advertiser', or third party contractors' use of such information" (Chicago Tribune, 2012: 1).

Table 2 shows what privacy policies say about how PII and non-PII information is received from users. Information can be obtained in a great variety of ways such as blogs, chats, credit card information, contests, sweepstakes, and special offers across all papers. The Chicago Tribune (2012) appears to have the most interesting statement with the following quote about collecting user information:

> "Certain third-parties who provide technical support for the operation of our site (our Web hosting service or ad serving services, for example), or who provide email management, third-party content, billing, processing, shipping, promotions management or other services also may access such information - Web hosting service - Ad serving services Email management - Third party content - Billing - Shipping - Promotions management - Or other services" (Chicago Tribune, 2012: 1).

It is unknown what "other services" are. This may mean that the Chicago Tribune is open to receive information about its readers from almost any other source.

Table 3 shows that information from readers can be used in a wide variety of ways. The newspapers perform a considerable amount of marketing research on their readers and provide data to advertisers. Customization of web content is common for the reader.

Privacy and freedom of speech have to be balanced. Privacy policies of newspapers are part of the effort to create this balance. According to Kirkpatrick (2010), who wrote The Facebook Effect, Facebook leaders think that freedom of speech is an opportunity for organizations and individuals to share relevant information to other organizations and individuals. Everyone should be given the opportunity to have their fifteen minutes of fame by sharing their life experiences, personal opinions, mutual friends, and great discoveries with others.

The problem with freedom of speech is that ethical issues are severely tested. Organizations should ensure that they collect, use, retain and disclose personal information in a confidential manner. According to Tapscott and Williams (2011: 1), "Unfortunately, the loss of privacy may lead to job losses for individuals because employers check their inappropriate online behavior. Identity theft is growing. Personal information involving biography, biology, genealogy, history, financial transactions, locations, and relationships of each individual can be revealed. Ultimately, in order to properly protect privacy, all of us will need to be vigilant about our own online behavior."

Future Research

Future research on privacy policies can be taken many directions. The easiest direction is to continue analyzing websites for their readability and their privacy features just like the current paper has done. While the current study has investigated the top ten newspapers in the United States, future studies can investigate more regional papers.

Privacy policies in these papers would probably not be as comprehensive as the top ten papers. Only the New York Times might be considered comprehensive in its privacy policy among the top ten papers. It is the only privacy policy to receive the TRUSTe (2012) award for quality among the top ten papers.

Future research also can investigate the privacy policies of international papers just as the Kaupins and Reed (2012) study started. That study investigated the top twelve papers in Latvia, Lithuania, and Estonia and found that in some of the papers, there were no privacy policies, especially in the regional editions.

Limiting privacy policy research to newspapers is not necessary when there are many industries to investigate. Examples include websites associated with magazines, universities, retail stores, manufacturers, and others actively engaged in consumer communications.

Further research also can investigate people's opinions of the privacy of various websites based on their experiences with the websites. There could be major differences between actual policies and peoples' perceptions of what is going on with the websites.

Conclusion

The top ten newspapers have created policies that have language that is more complicated than a typical reader would read. They have allowed themselves to collect data from a wide variety of sources and send the information to third parties who in turn can use the information for a wide array of purposes. A majority of third parties use these newspapers sites to collect PII. The use of your PI and PII collected by third parties are protected under the third party's privacy policy, not the newspapers. Newspapers state they may share some or all of your PII with their divisions, affiliates, vendors providing contractual services, sponsors of promotions, advertisers on their web sites, and third parties.

Also, newspaper privacy policies state if you do not accept their terms and conditions of their newspapers privacy policy, you will not be able to access their site. Regarding cookies, you may disable these on the newspaper's site, but this may result in a less complete experience while using their sites. Newspapers state that the reason for gathering your PII is to provide you, the user, with a customized experience on our network of sites.

Protection of personal information should be made stronger and easier to understand to the normal person, in order to insure that privacy laws such as the Electronic Communications Privacy Act, Wiretap Act, Stored Communications Act, and related acts are obeyed. Beyond that, meeting the legitimate expectations of customers as regarding their privacy, including reasonable policies that are clearly communicated, is simply good business. It may the take collective effort of customers and ultimately politicians to change corporate privacy policies.

REFERENCES

Buckley, N. 2010. **Ethics in social networking sites**. Retrieved January 21, 2011 from http://social-networking. limewebs.com/ethics.htm.

Buzzle.com. 2012. **Ethical issues of internet privacy**. Retrieved December 22, 2010 from http://www.buzzle.com/ articles/ethical-issues-of-internet-privacy.html.

California Privacy Rights. 2003. California Civil Code Section 1798.83.

CAN_SPAM Act. 2003. 117 Stat 2699.

Chicago Tribune. (2011, October 19). **Privacy policy**. Retrieved August 15, 2012 from http://privacy.tribune.com/.

Children's Online Privacy Protection Act of 1998. (15 U.S.C. §§ 6501 et seq., 16 C.F.R. § 312).

Coldwey, D. 2012. **Examination of privacy policies shows a few troubling trends**. Retrieved August 28, 2012 from http://techcrunch.com/2011/11/30/examination-of-privacy-policies-shows-a-few-troubling-trends/.

Coleman, M., & Liau, T. 1975. A computer readability formula designed for machine scoring. **Journal of Applied Psychology**, 60(2), 283-284.

Computer Fraud and Abuse Act. 1986. 18 USC 1030.

Duboff, J. (2007, August 3). **The latest crime-busting tool: Facebook.com**. Newsweek. Retrieved August 3, 2007 from http://www.msnbc.msn.com/id/12209620/site/newseek/print/1/displaymode/1098/.

EF Cultural Travel BV v. Zefer Corp. (1st Cir. 2003).

Electronic Communications Privacy Act. (18 U.S.C. § 2701, et seq.).

Equal Employment Opportunity Act. (1972) 42 U.S.C. § 2000e, et seq.

4imn.com (2012). 2012 **Newspaper rankings: Top 100 newspapers in North America**. Retrieved August 17, 2012 from http://www.4imn.com/topNorth-America/.

Gramm-Leach-Bliley Act. 1999. Pub. L 106-102, 113 Stat. 1338.

Gunning, R. 1952. **The technique of clear writing**. New York, NY: McGraw-Hill.

Harlan, J. (2012, August 20). **The 4th amendment in 21st century America**. Retrieved August 25, 2012 from http://www.newsorganizer.com/article/the-4th-amendment-in-21st-cent-94d4a763f5200ac20236a283374407b3/.

Hedman, A. (January 2008). Using the SMOG formula to revise a health-related document. **American Journal of Health Education**, 39(1), 61–64.

Hodge, M. 2006. **Comment: The fourth amendment and privacy issues on the 'new' internet, facebook.com and myspace.com**. Southern Illinois University Law School Journal. 31, 95-122.

In re Toys 'R' Us, Inc., Privacy Litig. (N.D. Cal. 2001).

Internet Crime Complaint Center (2011). **2011 Internet crime report**. Retrieved August 30, 2012 from http://www.ic3.gov/media/annualreport/2011_ic3report.pdf.

Kaupins, G., & Reed, D. 2012. New media usage and privacy policies of newspaper websites of the Baltic States. **Current Issues of Business and Law**, 7(1), 27-45.

Kincaid, J., Fishburne, R., Rogers, R., & Chissom, B. 1975. **Derivation of new readability formulas (automated readability index, fog count, and Flesch reading ease formula) for Navy enlisted personnel**. Research Branch Report 8-75. Chief of Naval Technical Training: Naval Air Station Memphis.

Kirkpatrick, D. 2010. **The Facebook effect: Inside story of the company that is connecting the world**. New York: Simon and Schuster.

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002).

Los Angeles Times. (2011, October 19). Privacy policy. Retrieved August 15, 2012 from http://privacy.tribune.com/.

Mason, R. 1986. Four ethical issues of the information age. **MIS Quarterly**, 10(1), 5-12.

Mackenzie, J. (2009, February 4). **How to monetize social media in the hospitality industry**. Retrieved April 4, 2011 from http://www.hotelmarketingstrategies.com/how-to-monetize-social-media/.

Marcus, J. et. al. 2007. **Comparison of privacy and trust policy in the area of electronic communications**. Retrieved August 28, 2012 from http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/final_report_20_07_07_pdf.pdf.

Parrish, J. 2010. PAPA knows best: Principles for the ethical sharing of information on social networking sites. **Ethics of Information Technology**, 12(2), 187-193.

Philadelphia Inquirer. (2007, October 2). **Privacy policy**. Retrieved August 15, 2012 from http://www.philly.com/philly/about/terms_of_use/.

New York Daily News. (2012, May 2). **Privacy policy**. Retrieved August 15, 2012 from http://www.nydailynews.com/services/privacy-policy.

New York Post. (2011, November 11). **Privacy policy**. Retrieved August 15, 2012 from http://www.nypost.com/p/static/privacy_policy_PlyzvkFUzwURLgq0xv11cN.

New York Times. (2011, December 5). **Privacy policy**. Retrieved August 15, 2012 from http://www.nytimes.com/content/help/rights/privacy/policy/privacy-policy.html.

Privacycast.com. (2012, March 26). **Privacy policy comparison: Top five social networking apps**. Retrieved August 28, 2012 from http://privacycast.com/privacy-policy-comparison-top-five-social-networking-apps/.

Reliabilityformulas.com. 2012. **The Flesch grade level reliability formula**. Retrieved August 29, 2012 from http://www.readabilityformulas.com/flesch-grade-level-readability-formula.php.

San Francisco Examiner. (May 2010). **Scope of this privacy policy**. Retrieved August 15, 2012 from http://www.sfexaminer.com/info/privacy.

Senter, R., Smith, E. (November, 1967). **Automated readability index**. Wright-Patterson Air Force Base. p. iii. AMRL-TR-6620.

Supnick v. Amazon.com, Inc., (W.D. Wash. 2000).

Tapscott, D., & Williams, A. 2011. **Macrowikinomics: Privacy in the age of facebook**. Retrieved January 10, 2011 from http://www.huffingtonpost.com/dontapscott/post_1543_b_806523.html.

Timm, D., & Duven, C. 2008. Privacy and social networking sites. **New Directions for Student Servces**, 124, 89-101.

TRUSTe. 2012. **Data privacy management solutions**. Retrieved August 30, 2012 from http://www.truste.com.

United States vs. Jones. 2012. **Slip opinion**. Retrieved November 14, 2012 from http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf.

USA Today. (2011, February 15). **USA Today.com privacy notice**. Retrieved August 15, 2012 from http://www.usatoday.com/marketing/privacy-notice.htm.

Wall Street Journal. (2011, October 18). **The Wall Street Journal digital network and the Wall Street Journal, Barron's and SmartMoney print editions privacy policy**. Retrieved August 15, 2012 from http://online.wsj.com/public/page/privacy-policy.html?mod=WSJ_footer.

Washington Post. (2011, November 15). **Privacy policy**. Retrieved August 15, 2012 from http://www.washingtonpost.com/privacy-policy/2011/11/18/gIQASIiaiN_story.html.

Wiretap Act. (1986). 18 USC 1510-2522.

Gundars Kaupins is department chair and professor at Boise State. He received his Ph.D. in human resource management from University of Iowa and is certified as a senior professional in human resources (SPHR). His publications include over 300 articles in job evaluation, training and development, Baltic studies, and human resource ethics.

Christy Suciu is a special lecturer at Boise State. She has an MBA from Webster University. She teaches leadership skills and strategic perspectives and has research interests in design thinking.

Mark Buchanan is a professor at Boise State. He has an LLM in international law from University of Illinois, Urbana-Champaign and a JD from University of Nebraska Lincoln. He teaches international trade and investment law and business in society: Ethics, responsibility, and sustainability. His publications include articles in stakeholder analysis, corporate social responsibility, and international business transactions.