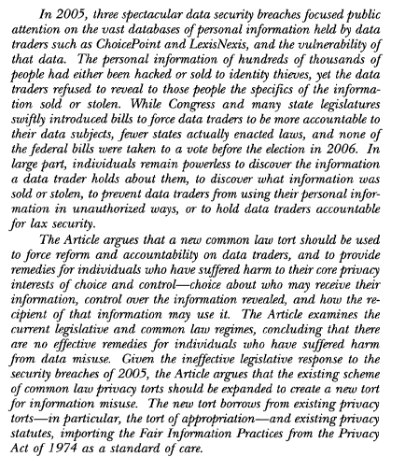
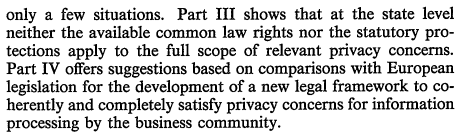
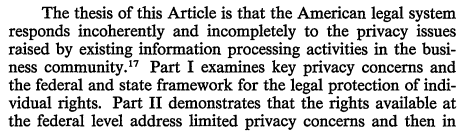
**5/15/20**

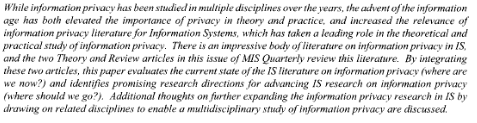
**[Google Scholar (“personal information privacy”)]**

* **PERSONAL INFORMATION PRIVACY SETTINGS OF ONLINE SOCIAL NETWORKS AND THEIR SUITABILITY FOR MOBILE INTERNET DEVICES**
  + Abstract
    - *Protecting personal information privacy has become a controversial issue among online social network providers and users. Most social network providers have developed several techniques to decrease threats and risks to the users’ privacy. These risks include the misuse of personal information which may lead to illegal acts such as identity theft. This study aims to measure the awareness of users on protecting their personal information privacy, as well as the suitability of the privacy systems which they use to modify privacy settings. Survey results show high percentage of the use of smart phones for web services but the current privacy settings for online social networks need to be improved to support different type of mobile phones screens. Because most users use their mobilephones for Internet services, privacy settings that are compatible with mobile phones need to be developed. The method of selecting privacy settings should also be simplified to provide users with a clear picture of the data that will be shared with others. Results of this study can be used to develop a new privacy system which will help users control their personal information easily from different devices, including mobile Internet devices and computers.*
  + DOI/Link
    - 10.5121/ijsptm.2013.2201
  + Link to Project
    - Shows external links to the use of mobile phones to ease of information posted online. It could be useful in establishing risks outside of the company misusing information, however, other studies would be more useful for the prioritized scope.
* **Reining in the Data Traders: A Tort for the Misuse of Personal Information**
  + Abstract
    - 
  + DOI/Link
    - <https://heinonline.org/HOL/P?h=hein.journals/mllr66&i=146>
  + Link to Project
    - This article shows how Data obtained from customers and held by companies are not protected well. Furthermore, hacks on these servers put customer information at risk as it is unprotected/misused. Could help later to show that information obtained legally should be protected/monitored especially if it is “sold”
* **Unwillingness to pay for privacy: A Field Experiment**
  + Abstract
    - *We measure willingness to pay for privacy in a field experiment. Participants bought at most one DVD from one of two competing online stores. One store consistently required more sensitive personal data than the other, but otherwise, the stores were identical. In one treatment, DVDs were one Euro cheaper at the store requesting more personal information, and almost all buyers chose the cheaper store. Surprisingly, in the second treatment when prices were identical, participants bought from both shops equally often.*
  + DOI/Link
    - <https://doi.org/10.1016/j.econlet.2012.04.077>
  + Link to Project
    - People would rather provide personal info than pay for services to protect personal information. Lack of care about personal information on the internet causes people to overlook privacy policies and other vital information despite personal consequences. It could be useful to help teach others to stop allowing such information to become readily available.
* **Privacy in the Information Economy: A Fortress or Frontier for Individual Rights**
  + Abstract
    - 

|  |
| --- |

* DOI/Link
  + <https://heinonline-org.ezproxy.lib.vt.edu/HOL/Page?collection=journals&handle=hein.journals/fedcom44&id=205&men_tab=srchresults#>
* Link to Project
  + US law does not adequately protect the consumers from the businesses and newer laws need to enacted to better protect the people. Could help show that improvements need to be made to better protect everyone. Especially in cooperation with the evidence we produce.

# **State of the Information Privacy Literature: Where are We Now And Where Should We Go?**

* + Abstract
    - 
  + DOI/Link
    - 10.2307/41409969
  + Link to Project
    - Shows that research should be expanded upon this topic which has multiple similarities to our scope. Furthermore, this literature search can help be a platform from which we can expand our research off of.

**5/21/20**

* **FaceCloak: An Architecture for User Privacy on Social Networking Sites** 
  + Abstract
    - *—Social networking sites, such as MySpace, Facebook and Flickr, are gaining more and more popularity among Internet users. As users are enjoying this new style of networking, privacy concerns are also attracting increasing public attention due to reports about privacy breaches on social networking sites. We propose FaceCloak, an architecture that protects user privacy on a social networking site by shielding a user’s personal information from the site and from other users that were not explicitly authorized by the user. At the same time, FaceCloak seamlessly maintains usability of the site’s services. FaceCloak achieves these goals by providing fake information to the social networking site and by storing sensitive information in encrypted form on a separate server. We implemented our solution as a Firefox browser extension for the Facebook platform. Our experiments show that our solution successfully conceals a user’s personal information, while allowing the user and her friends to explore Facebook pages and services as usual.*
  + DOI/Link
    - [**https://cs.uwaterloo.ca/~uhengart/publications/passat09.pdf**](https://cs.uwaterloo.ca/~uhengart/publications/passat09.pdf)
  + Link to Project
    - Kind of a final product or end note of what we would be trying to accomplish. Information obtained from this article could help us with the setup phase. Extension that would prevent information from being leaked to facebook without prior authorization (does break TOU)

# ***What Anyone Can Know: The Privacy Risks of Social Networking Sites***

* **Information Revelation and Privacy in Online Social Networks**
  + DOI/Link
    - <https://dl.acm.org/doi/pdf/10.1145/1102199.1102214>
  + Abstract
    - Participation in social networking sites has dramatically increased in recent years. Services such as Friendster, Tribe, or the Facebook allow millions of individuals to create online profiles and share personal information with vast networks of friends - and, often, unknown numbers of strangers. In this paper we study patterns of information revelation in online social networks and their privacy implications. We analyze the online behavior of more than 4,000 Carnegie Mellon University students who have joined a popular social networking site catered to colleges. We evaluate the amount of information they disclose and study their usage of the site’s privacy settings. We highlight potential attacks on various aspects of their privacy, and we show that only a minimal percentage of users changes the highly permeable privacy preferences.
  + Link to Project
* **Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace**
  + DOI/Link
    - <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1849&context=amcis2007>
  + Abstract
    - It is not well understood how privacy concern and trust influence social interactions within social networking sites. An online survey of two popular social networking sites, Facebook and MySpace, compared perceptions of trust and privacy concern, along with willingness to share information and develop new relationships. Members of both sites reported similar levels of privacy concern. Facebook members expressed significantly greater trust in both Facebook and its members, and were more willing to share identifying information. Even so, MySpace members reported significantly more experience using the site to meet new people. These results suggest that in online interaction, trust is not as necessary in the building of new relationships as it is in face to face encounters. They also show that in an online site, the existence of trust and the willingness to share information do not automatically translate into new social interaction. This study demonstrates online relationships can develop in sites where perceived trust and privacy safeguards are weak.
  + Link to Project
* **Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression**
  + Abstract
    - The explosion in social networking sites such as MySpace, Facebook, Bebo and Friendster is widely regarded as an exciting opportunity, especially for youth. Yet the public response tends to be one of puzzled dismay regarding, supposedly, a generation with many friends but little sense of privacy and a narcissistic fascination with self-display. This article explores teenagers’ practices of social networking in order to uncover the subtle connections between online opportunity and risk. While younger teenagers relish the opportunities to continuously recreate sa highly decorated, stylistically elaborate identity, older teenagers favour a plain aesthetic that foregrounds their links to others, thus expressing a notion of identity lived through authentic relationships. The article further contrasts teenagers’ graded conception of ‘friends’ with the binary classification of social networking sites, this being one of several means by which online privacy is shaped, and undermined, by the affordances of these sites.
  + Link
    - <http://eprints.lse.ac.uk/27072/1/Taking_risky_opportunities_in_youthful_content_creation_%28LSERO%29.pdf>
  + Link to Project
* **Privacy Violations Using Micro-targeted Ads: A case study**
  + Link
    - <https://theory.stanford.edu/~korolova/Privacy_violations_using_microtargeted_ads.pdf>
  + Link to Project
    - Exploited ad systems compromised personal information security. Informaiton that users have expliticed not given consent on are handed out to obtain more relevant ad information. Needs to be better layer between private information and public infromation
* **Privacy Protection Strategies on Facebook**
  + Link
    - <https://www.tandfonline.com/doi/abs/10.1080/1369118X.2013.777757>
* **Toward a Framework for Detecting Privacy Policy Violations in Android Application Code** 
  + Abstract
    - Mobile applications frequently access sensitive personal information to meet user or business requirements. Because such information is sensitive in general, regulators increasingly require mobileapp developers to publish privacy policies that describe what information is collected. Furthermore, regulators have fined companies when these policies are inconsistent with the actual data practices of mobile apps. To help mobile-app developers check their privacy policies against their apps’ code for consistency, we propose a semi-automated framework that consists of a policy terminologyAPI method map that links policy phrases to API methods that produce sensitive information, and information flow analysis to detect misalignments. We present an implementation of our framework based on a privacy-policy-phrase ontology and a collection of mappings from API methods to policy phrases. Our empirical evaluation on 477 top Android apps discovered 341 potential privacy policy violations
  + Link
    - <https://dl.acm.org/doi/pdf/10.1145/2884781.2884855>
  + Link to Project
    - Created a program that evaluates app policies and determines whether they contain violations of personal privacy. Apps contained a lot of them. Stronger than Keyword searches. Explains that privacy policy is inaccurate in how they collect information. While they have legal obligation companies do not seem to disclose most of the info