5-2011

Privacy Law and the Internet using Facebook.com as a Case Study

Amelia D. Grubbs
University of Tennessee, Knoxville: College of Communication and Information, Journalism and Electronic Media Department, Student, agrubbs1@utk.edu

Privacy Law and the Internet using Facebook.com as a Case Study

Amelia Grubbs

Journalism and Electronic Media Major

Chancellor's Honors Program

Senior Honors Thesis Paper

Advisor: Dr. Barbara Moore

Spring 2011

OUTLINE: Privacy and the Internet using Facebook as a Case Study

I. Introduction

1. Brief history on privacy law

2. Introduce controversy of privacy on the Internet

II. Privacy Tort Law: 4 Torts

1. Intrusion

- Including secret surveillance, traditional trespass, consent to enter is exceeded

2. Public disclosure of private facts

-Publication of private information that is highly offensive to a reasonable person and is not a matter of legitimate public concern

3. False light

-The publication of facts placing the plaintiff in a false light that is highly offensive to a reasonable person and if the issue is of public concern, published with actual malice

4. Appropriation

-Right of publicity, right to control the commercial exploitation of your name and likeness

III. Various Privacy Issues with the Internet and Regulations

A. E-commerce, online fraud, and online profiling (FTCA)

-Data bank problems

-5 basic elements of an online privacy policy by FTC

1. Notice/awareness
2. Choice/consent
3. Access/participation
4. Integrity/security
5. Enforcement/redress

B. Children online (COPPA)

-Enhance parental involvement in child's online activities to protect child's privacy

-Help protect child safety on social network and chat sites

-Maintain security of child's personal information collected online

-Limit collection of personal information from child without parental consent

C. Online Financial Institutions (Gramm-Leach-Bliley Act and Fair Credit Reporting Act)

-Protects nonpublic personal information (assets, credit history, names, addresses, phone numbers, account numbers) of consumers of financial products and services provided by financial institutions

-Requires institutions to provide notice to consumers regarding privacy policy and practices

-Limits ability to give third parties consumer info, and also limits reuse and redisclosure of consumer information by third parties

D. Healthcare online (HIPAA)

-Medical records and information kept private by insurance companies, healthcare clearinghouses, and healthcare providers

IV. Privacy Issues Specifically Surrounding Facebook.com (case study)

A. Data mining

-Intrusion and public disclosure of private facts torts

- Sharing user information with advertisers

-Popular applications made for the social network, such as FarmVille, Texas HoldEm Poker and FrontierVille, have been sending users' personal information to dozens of advertising and Internet monitoring companies.

-Case law or precedent applicable?—AOL, Apple

-Prediction of court ruling

B. Protection from cyber bullying, trolling, and false identities/identity theft?

-Intrusion and false light torts

-Case law or precedent applicable?-- Google

-Prediction of court ruling

C. Safe for minors?

-Intrusion tort

-Case law or precedent applicable?—Google, EchoMetrix

-Prediction of court ruling

D. Terms of Use and Privacy Agreement (electronic contracts)

-Intrusion and appropriation torts

-Cannot voluntarily delete account, and once deleted facebook.com owns rights to your images and profile content

- Facebook does not take adequate steps to protect user privacy: firms are using it for marketing purposes

-Should there be an opt out option within privacy settings and contract or should that be the default and users decide to opt in?

-Case law or precedent applicable?—Google

-Prediction of court ruling

E. Users disclose too much, and university administrators are using Facebook for disciplinary purposes

-False light and appropriation torts

-Case law or precedent applicable?—Yahoo, YouTube users or site in trouble?

-Prediction of court ruling

F. Spyware

-Intrusion and disclosure of private facts torts

- Third parties are actively seeking out end-user information using Facebook, and thus intruders are exploiting security holes

-Case law or precedent applicable?—Interclick, Apple

-Prediction of court ruling

V. Suggestions

A. What should the law do?

B. Ways to achieve the right balance of law:

1. Refurbishing the Appropriation Tort
   -Other torts that may help
2. State regulation (Delaware where Facebook is incorporated vs. Tennessee for example, problems with jurisdiction like for subpoenas from one state to another)
3. Federal regulation
4. Self regulation
5. Consumer awareness

VI. Conclusion

1. Brief summary of evolution of privacy law

2. Summary of Facebook dilemmas

3. Summary of suggestions and prediction of future in Internet privacy laws

I. Privacy Laws—a brief history

On April 25, 1995, following the Oklahoma City bombing on April 19, 1995, an unidentified person posted on AOL's "Michigan Military Movement" bulletin board an advertisement for "Naughty Oklahoma T-Shirts" which listed the notice to be from Ken ZZ03, giving Kenneth Zeran of Seattle's telephone number. The listing was a hoax designed to generate outrage at the supposed seller. When Zeran found out about the posting, he notified AOL by telephone and letter requesting that the posting be deleted and that there be a notice on the bulletin board saying that the post was a sham. The posting remained, however, or was reposted with slightly different screen names, but always using Zeran's phone number, for the following week. Because AOL failed to delete the posting in a swift manner and because it failed to prevent reposting through blocking the user's ISP, Zeran's phone line was tied up with harassing phone calls and death threats. He suffered further humiliation when a radio broadcast in Oklahoma City attributed him to the posting on May 1, 1995. At this point, Zeran's house was placed under protective surveillance, and he was unable to use his telephone, as the threatening calls were coming in approximately every two minutes. This continued until at least May 15, by which time the number of calls reduced to only approximately 15 per day.[39]

Zeran sued AOL for negligence as a distributor for failure to exercise a standard of care to protect Zeran from the foreseeable consequences of the fake posting. The courts sided with AOL citing the Communications Decency Act of 1996, Section 230. The CDA protects online service providers and users from actions against them based on the content of third parties, stating in part that "No provider or user of an interactive computer service shall be treated as

the publisher or speaker of any information provided by another information content provider." Effectively, this section immunizes both ISPs and Internet users from liability for privacy violations committed by others using their website or online forum, even if the provider fails to take action after receiving actual notice of the harmful or offensive content.[39]

Technology has transformed the way Americans view and interact with the world. We are in the information era, and most everything we could possibly want to know is just a click away. With that freedom of information, however, comes a price—our private information is now some of the most freely accessed information on the Internet. As Americans, we value our freedoms and civil liberties, but within that is a controversy: we believe in freedom of expression and the free flow of information, yet we also highly value the right to keep personal information private.[4]

The Internet presents a new challenge to our beliefs and rights. The Internet produces a new set of challenges with privacy regulation as well, which adds to the difficulty of control. Personal information is easily transmitted via the Internet, and corporate websites recognize this. They use marketing tools to collect personal information of commercial value from usually unsuspecting users.[4]

Privacy concerns have existed since the founding of this country, and these issues are reflected in the Bill of Rights protection of the home, private papers, religion, association, and conscience. Because of the rise of photography and popular journalism in the 19th century, many began to call for even greater protections of personal privacy. During the 20th century,

legal rights of privacy became a significant part of both private and public law. Privacy rights appeared as tort law and other state law, constitutional law, and federal statutes.[8]

Now, in the 21st century because of reliance on electronic, computer, and telephone surveillance, there is a want for aggressive data protection and privacy regulation. The private sector along with Congress and the Federal Trade Commission have now begun to heed these calls, however, many of these laws are difficult to enforce due to the broad body of laws that sometime overlap and sometime contradict one another.[8]

This paper will first discuss the main body of legislation used to enforce privacy: the four privacy torts. It will also discuss the legislation on the Federal Trade Commission Act, the Children's Online Privacy Protection Act, the Gramm-Leach-Bliley and Fair Credit Reporting acts, as well as the Health Insurance Portability and Accountability Act. This paper will then discuss issues of privacy law on the Internet and the troubles of regulating data mining, identity theft and cyber bullying, minors' safety, electronic contracts, amount of user disclosure, and spyware using Facebook.com as the case study. To conclude, the paper will entail suggestions on how to improve regulation of these issues via current state or federal laws or by enacting new policies. The main question this paper attempts to answer is how much legal protection does the average consumer get on the Internet and how much does the consumer actually need?

II. Privacy Tort Law—4 Torts

Privacy is the right to be let alone and to be free of unwarranted publicity. The main body of laws that protect personal privacy are the four privacy torts: intrusion, public disclosure of private facts, false light, and appropriation (Restatement of Torts (2d) Sections 652B, C, D,

and E 1964). The state of Tennessee recognizes all four torts, however some states only recognize some of them, and four states don't recognize them at all.

A. Intrusion includes secret surveillance, traditional trespass, and when consent to enter is exceeded. Traditionally, the tort of intrusion comes from the physical or visual intrusion into the personal or private space of the plaintiff, typically from being spied upon, taped or photographed, or their home entered without consent. Internet intrusion encompasses activities like hacking and spamming (mass distribution of unsolicited or unwanted advertisements or emails).[4]

B. Public disclosure of private facts is the publication of private information that is highly offensive to a reasonable person and is not a matter of legitimate public concern. A defendant invades another's privacy when he or she publicly discloses private facts about the plaintiff, with private facts normally encompassing family, sexual, medical, financial, and other highly personal topics. The main defense against this privacy violation claim is that the information at hand was newsworthy and thus its disclosure was not illegal. To test for newsworthiness one would need to look at whether the information disclosed was of legitimate public concern, which is determined by the information's social value, the depth of intrusion into private facts, and the extent to which the plaintiff voluntarily put themselves in the public eye.[4]

C. False light is the publication of facts placing the plaintiff in a false light that is highly offensive to a reasonable person and if the issue is of public concern, published with actual malice. This tort is very similar to the defamation claim; however it covers those who are in the public eye. Some states even treat it as the same, such as in California. It

most often happens when a false impression can be derived from something other than an explicit statement, like a photograph or video for instance: the picture is shown at the same time or in conjunction with an unrelated statement, which gives the impression that the statement is about the featured individual. The use of frames and hyper linking on one website to another could give rise to similar false light claims. The use of individual's photos placed on the web by a website also could fall under the false light tort.[4]

D. Finally, appropriation is the right of publicity or the right to control the commercial exploitation of your name and likeness. Under various state laws, permission is needed for the commercial exploitation of the name, image or personal attribute of an individual, and in some cases even dead celebrities. Without receiving proper release by a person whose name, image, or likeness is used in any commercial (i.e. for profit) capacity on the web (websites, advertisements, promotions, etc), there could be a violation of the appropriation tort online.[4]

III. Various Privacy Issues with the Internet and Regulations

During the last five decades since the Restatement of Torts (652 B-E), the US has generally developed privacy protections on a sector by sector basis instead of comprehensive privacy legislation[7]:

A. E-commerce, online fraud, and online profiling (FTCA)

The main privacy issue on the Internet comes from the growing practice of data collection. Internet commerce relies heavily on specific and detailed data about

consumer habits on the web. Many websites use “cookies” and other tracking technologies to record the activities of users who visit their sites. When a user is on the Internet, each site visited and each page viewed within a certain site are logged by the user’s Internet Service Provider. Most ISPs maintain a record of a user’s email communications and other online activities like the websites visited, ads viewed, and purchases made, and so on—this is all termed as *click stream data*. Individual websites also can track user activities with their “cookie” technology. “Cookies” allow the World Wide Web server to keep track of what the user did when a person was on the said site. The cookie can also remember the name and password the server assigned to the person during their last visit. A cookie does identify an individual’s computer since it can distinguish one computer from another, however, it doesn’t know the actual identity of the person using the computer—although some can identify the server or ISP of the user).

Cookies theoretically enhance the browsing experience because they send the server a list of the user’s selected preferences, thus personalizing the site for the user’s future visits. Cookies allow websites to develop profiles of visits to the site as well as individual preferences, which is highly valuable when marketing the site to advertisers on the Internet. The question is—is this invasion of privacy? Many people unknowingly have cookies on their computers, without giving any sort of consent. Unless a user’s preferences are set on the browser to notify the user when a cookie is sent, cookies enter the computer unannounced and unsolicited. Many ISPs and browsers do allow users to be alerted when a site sends a cookie or to block cookies altogether.

There is also a limitation of disclosure on this information that websites and ISPs record. The Electronic Communications Privacy Act of 1986 limits user information that ISPs can give to the government. A government entity must provide a subpoena, warrant, or court order to get information stored by the ISP. The problem with even this comes when a state court issues a subpoena, warrant, or court order for the information and that state isn't where the ISP is incorporated—by law it is actually then illegal to send user information across borders as such, further complicating the matter. The act, however, does not prohibit disclosure of user information to non-government entities.[4] Section 5 of the Federal Trade Commission Act allows the FTC to prohibit "unfair or deceptive acts or practices in or affecting commerce." The FTC has historically applied a three part test to decide whether an act is unfair or not:

1. Is it a practice likely to cause substantial consumer injury?
2. Is the injury reasonably avoidable?
3. Is the practice outweighed by countervailing benefits to consumers or competition?

Inadequate data security is considered unfair by the FTC, along with a website not following its own posted web policy, which the FTC also considers deceptive.[8] The FTC also has privacy guidelines for fair information practices in consumer transactions. The commission surveyed government studies from both the U.S. and other countries, and concluded that it was possible to generalize core principles of fair information practices. The five basic elements of the FTC online fairness policy include

1. *Notice/awareness* of an entities information practices

2. *Choice/consent* with respect to how information about them is collected, used, and disseminated

3. *Access/participation* to information about them and store in an entity

4. *Integrity/security* that a data collector has taken appropriate steps to ensure the safekeeping of any information collected

5. *Enforcement/redress* to ensure compliance with these principles when they are adopted in practice codes or guidelines.[3]

The Electronic Communications Privacy Act also aids the FTC, by prohibiting the interception of communications while in transit or when it is stored on a network. [3]

B. Children online (COPPA)

The Children's Online Privacy Protection Act of 1998 imposes requirements on websites that obtain personal information from children under the age of 13. The FTC enforces the regulations for this act, and requires that any website or online service directed to children post directly on their website a notice saying what information is being collected, how the information is used by the website, and what the website's operator disclosure practices are.[4] Under FTC regulation, the sites must also obtain verifiable parental consent for the collection, use or disclosure of personal information from children. The sites must also provide information to parents when they request it. The FTC prohibits a website from conditioning a child's participation on the site where the child has to disclose additional personal information, even if it is reasonably necessary to do so in order to participate on the site. Websites also have to establish and maintain reasonable procedures to protect the "confidentiality, security, and

integrity of personal information collected from children."[3] COPPA enhances parental involvement in a child's online activities to protect the child's privacy, helps protect children on social network and chat sites, maintains security of a child's personal information collected online, and limits collection of personal information from a child without parental consent. [6]

In 1999, the FTC brought charges against GeoCities, which was operating a virtually community website made up of individuals' home pages. GeoCities was accused of collecting personal information from kids without parental consent or notice. The case arose out of concern for child privacy on the Internet; however, the case's results have generally applicability to most online sites and their privacy conditions. The FTC set out an order of what GeoCities' privacy statement should look like, where it should appear, and what it should accomplish:

1. What information is being collected (i.e. name, address, email, age, interests)
2. Its intended use(s)
3. The third parties to whom it will be disclosed (i.e. advertisers for consumer products, mailing lists, the general public)
4. The consumer's ability to obtain access to or directly access this information and the means by which to do so
5. The consumer's ability to remove directly or have the information removed from databases and the means by which to do so
6. The procedures to delete personal identifying information from the databases and any limitations to such deletion

The GeoCities order does not bind any other entity but GeoCities, but the privacy statement requirements the FTC set forth for them have been a model for other sites to model their privacy agreements on.[4]

C. Online Financial Institutions (Gramm-Leach-Bliley Act and Fair Credit Reporting Act)

The Fair Credit Reporting Act prohibits the disclosure of information from a person's credit file, like the credit history or employment data without consent. However, nonfinancial information found in a person's credit document such as name, aliases, birth date, social security number, current and prior addresses, and phone numbers, is not protected by this act.[3] Title V of the Financial Services Modernization Act (Gramm-Leach-Bliley) requires that banks, investment companies, insurance companies, and other financial providers give consumers notice when they utilize data sharing and collection policies and provisions.

Customers may opt out of certain information sharing practices with affiliated and non-affiliated businesses.[7] The GLB Act protects nonpublic personal information (assets, credit history, names, addresses, phone numbers, and account numbers) of consumers of financial products and services provided by financial institutions. It also requires institutions to provide notice to consumers regarding privacy policy and practices. The GLB Act also limits the ability to give third parties consumer info and as well as limits the reuse and redisclosure of consumer information by third parties. [6] Other financial privacy acts include the Electronic Funds Transfer Act, which requires that contracts with consumers for electronic funds transfers inform the consumers when and how their information may be disclosed, and the Computer Fraud and Abuse

Act, which allows for civil and criminal charges to be issued when someone breaks into a computer network, or exceeds authorized access, and obtains financial, medical, or other personal information of that nature.[3]

D. Healthcare online (HIPAA)

The Health Insurance Portability and Accountability Act regulates access to healthcare information in possession of physicians, hospitals, insurers, researchers, and the government. It sets data security transmission standards as well for health information. State laws mostly protect health information, with HIPAA only partly preempts state health privacy statutes. Many states have specific statutes regulating particular types of information like HIV testing data or genetic information.[7] Healthcare entities, with few exceptions, must provide a written notice on their privacy practices to any individual using their services. These healthcare firms may not go against any of their stated privacy practices per HIPAA. The basic elements of the mandatory privacy statement include:

1. Header—giving specific language to the nature of the notice (i.e. "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW CAREFULLY."[6]).
2. Uses and disclosures—describing all uses and disclosures of protected healthcare information that the entity is permitted or required to make and a statement saying all other uses of the information must come with express authorization of the individual.

3. Individual rights—describing patient rights under HIPAA and how they can exercise those rights.
4. Emphasis: covered entity's duties—stating that the entity is required by law to maintain the privacy of the patient, to provide a notice of its legal duties and practices, and to abide by the current requirements in the said notice. If the healthcare entity wishes to revise its privacy notice or policies, it must make a statement on that and how it will provide individuals with a revised notice.
5. Complaints—informing individuals how they can lodge complaints with the entity and they can file a complaint with the Department of Health and Human Services if their privacy has been violated.
6. Contact person—indentifying a contact person from whom the individual can obtain additional information about the notice.
7. Effective date—showing the date the notice went into effect.
8. Optional elements—describing privacy practices that are even more limited than those permitted by HIPAA.
9. Revisions to the notice—reserving the right to make changes to the notice, if the entity so chooses to change its privacy practices over time.

If an individual has given consent to receive electronic notification, this notice can be sent by email instead of printed out or sent my mail. An entity that maintains a website with information about the entity's services or benefits must prominently post this privacy notice on their website.[6]

IV. Privacy Issues Surrounding Facebook.com

This paper will use Facebook.com as its case study because of the vast amount of people who use the social networking site, and thus the vast effects it has on the greater populations' privacy concerns. Facebook.com was created in 2004 by Harvard University student Mark Zuckerberg. In just a few weeks after its launch, more than half of the undergraduate study body at Harvard had a profile. The site then started allowing other students from other college campuses to join the network, and by the end of 2004, more than one million students had pages. It continued to expand in 2005, adding thousands of colleges worldwide as well as around twenty-five thousand high schools. Over twenty thousand new accounts are activated each day, with over 90 percent of people on college campuses having a Facebook account. What is surprising, however, is the amount of information people are willing to disclose on the site: 90.8 percent have a profile picture, 87.8 percent show their birthday, 39.9 percent give a phone number, and 50.8 percent list their current address. In addition, almost all profiles fully identify people with their first and last names.[10]

The social networking site has been hit with a vast amount of privacy suits over the past few years since allowing advertisers on the site to generate revenue. Issues and complaints have ranged from data mining, identity theft and cyber bullying, legal-minor safety, the site's privacy agreement and terms of use, user disclosure discretion, to spyware. As with most any other company, Facebook wants to be seen as a champion of people's privacy online. Facebook uses people's identities online, which is the main aspect that makes the company different: most users register with their real names, which means that Facebook has more identifying

information than most other sites. Facebook can thus use that "privacy" (its access to people's private data) to its advantage.[23]

A. Data mining

Facebook.com has been accused of collecting and analyzing site content without user consent or knowledge, quite frequently over a vast number of ways. In late 2007, Facebook put in an advertising system called Beacon. It took the activity users conducted on other websites and sent that information back to Facebook. The idea was that all a user's friends would see their actions on their page with a link so that the friends could follow suit—something very useful for advertising companies. This of course, was very controversial, especially since it monitored all activity—not just when one was signed into Facebook.

A class action lawsuit was lodged against the company on behalf of all Facebook users, claiming that the system was too difficult for users to opt out of and it wasn't telling them the entire truth. In 2009, Facebook settled that suit out of court for a mere $9.5 million and also promised to shut down the Beacon system completely.[23] Facebook set off complaints again in December 2009 by changing some of its default settings to "share-everything." Then, in April 2010 the social networking company made another set of changes, one of which was the "instant personalization" program, where it shares users' names and other data with Yelp, Pandora and Microsoft Docs. Users can opt out, but if they don't do so their information is shared by default.[19] In October 2010, Facebook was sued by users for applications or games that one can join as a member on Facebook and play with other members of the social networking website. Popular

applications made for the social network, such as FarmVille, Texas HoldEm Poker and FrontierVille, have been sending users' personal information to dozens of advertising and Internet monitoring companies. Makers of Facebook applications were sending user ID numbers to outside firms. These numbers then could be used to look up people's names and in some cases other information.[24]

The problem is that these are all databank systems. Facebook is letting third parties run ads and collect information from its users, as well as sharing its users' information with other third parties for revenue. What is considered a third party? Any business that Facebook is working with to make a profit, including outsourcing, partnering, and co-branding relationships is a third party. Third parties also can include affiliates, which are separate legal entities. Failing to disclose in a privacy policy that a web site is disclosing users' personal information to third parties can lead to class-action lawsuits and multi-million dollar settlements, as we have seen with Facebook.[7]

The Privacy Act of 1974 mandates that only information relevant to a specific purpose can be collected and that it be accurate, complete, and up to date. Also, the act forbids external disclosure of an individual's personal data without the consent of the user. The act, however, includes no specific enforcement of these mandates, and leaves disclosure policies up to the agencies themselves. An agency, like Facebook, can decide that disclosure is compatible with the purpose for which the information was collected if it establishes that these disclosures are a "routine use."

The Organization for Economic Co-operation and Development in the 1980s created guidelines for privacy and data flow, which should be followed in the case of

data mining. There should be a limitation on collection of personal data: it is lawful and has the knowledge or consent of the participant. The data collected should be relevant and necessary for data collection purposes. The purposes for which the collection of data is being used should be spelled out and the agency should limit itself to those purposes. Personal data should not be exposed for any other purposes or to any other party, except under authority of the law. There should be reasonable protection of the collected personal data. The agency should be open with individuals on the collection of their personal data and should be stated in some sort of privacy policy. Individuals should have the right to obtain from the data controller the information related to them and should receive it within a reasonable time frame. The data controller should be accountable for the safe keeping of this stated information.

In 1997, the Open Profiling Standard was proposed in safeguarding the information websites gather from their users. This policy shows a blend of commercialism and interest for privacy: (1) control by source, (2) informed consent, and (3) appropriate-value exchange. The parties responsible for creating information (i.e. individual users and the entity that is gathering the information) should control its dissemination. Parties requesting access to a user's information must receive consent from the sources before collecting and using the data, and must explain how it will be used. Finally, no party should collect information about a person without offering them something of value in exchange (i.e. Facebook users' information is collected in exchange of use for a free social networking site).[11] These all, of course, are just

guidelines and proposals that have been made in attempts to solve these data mining issues, not laws.

The privacy torts that could help control data mining and that could be used in a lawsuit would most likely be *intrusion* and *public disclosure of private facts*. Intrusion would cover the gathering of the information activities by Facebook, when a user is right to believe that they have some expectation of privacy. This is especially the case when they are not logged onto Facebook, yet data mining systems like Beacon are used to obtain information as a user surfs the net or checks their email and all of this is unknowingly being tracked. Public disclosure of private facts is when a users' information is widely disclosed. Unlike defamation, the public-disclosure tort protects against truths being dispersed. Without user consent or knowledge to their information being shared with third parties or that third parties are obtaining user information, Facebook could also be sued under the public-disclosure tort. The issue being, however, that courts are uneasy about privacy torts and thus many people suing under privacy torts frequently lose their cases because the court does not recognize a privacy violation because of its narrow understanding of privacy law. [10]

Applicable Case Laws: In July 2006, AOL came under fire for releasing search data of its users onto the Web—followed by a class action law suit. According to the New York Times, the identity of one of the 650,000 supposedly anonymous users that used AOL to conduct 21 million Internet searches was found out from those searches.[15] The information posted included personal information as well as addresses, credit card numbers, phone numbers, social security numbers, and passwords. According to the

class action suit filed on behalf of members who had their information posted, their "personal struggles with various highly personal issues, including sexuality, mental illness, recovery from alcoholism, and victimization from incest, physical abuse, domestic violence, adultery, and rape," were made public. Time Warner, owner of AOL, got the case thrown out because it was filed in California, stipulating all legal disputes had to go through Virginia courts because of AOL's customer agreements.

A ruling by a federal appellate court in January 2009 reversed that decision, saying California residents could sue AOL over invasion of privacy in California rather than 'in courts of Virginia' as stipulated by AOL.[16] Another lawsuit was filed in December 2010 against Apple and at least eight mobile app developers for allegedly transmitting user information to advertising networks without the consent of owners of its mobile products, like the iPhone and iPad. The suit claims that apps can personally identify each user through a combination of each phone's Unique Device ID (UDID) which cannot be changed, plus other data harvested from user activity. Because it has a "class action" status, more plaintiffs (theoretically any iPhone user) could get in on the suit, and more app developers could be added.[37] The outcomes of cases like these are very important to corporate websites like Facebook because they will determine how the sits carry on business from that point forward.

Direction of court ruling: If Facebook has stated in its privacy policy and user agreement that it can give Facebook users' information to third parties and Facebook has specifically named those third parties in the agreement, then Facebook should be safe for now (until new rulings or new laws). And if third party companies are being

used by Facebook users and users agree to the third parties' user agreements, then they also have very little chance of being sued successfully. The issue comes with technologies like Facebook's use of Beacon. The social networking site used this tracking system on all of its users, even the ones who signed up before it was initiated and thus before it was in Facebook's user agreement and privacy policy. This is when corporate websites need to be careful before initiating new programs within the site that affect their users. Suits against violation of privacy due to breakage of a contract have historically been much more successful that just suits on the basis of a violation of a privacy tort. Plus, many courts have the view that if users have agreed to the privacy policy of an online company, then they have waived whatever rights to privacy they would normally expect.

B. Protection from cyber bullying, trolling, and false identities/identity theft?

Facebook's "advanced search" allows one to search the database of users using any of the fields in a profile. For example, one can search for junior females at the University of Tennessee in Knoxville that enjoy watching basketball. The problem with this is that when people "hide" their profile page, they are expecting that their information is then private. However, this information is not actually secure unless the user also excludes their profile from searches. Other users are free to download photos one is tagged in and also create a fake profile of someone, as well. Facebook has been slow to remove false profiles from their sites, even after repeated complaints.

Facebook users at one point also could not voluntarily delete their accounts—they could only deactivate them, but all that information was still there on Facebook

ready to be reactivated again. Now users can delete their profiles, but they must go through each photograph, wall post, and so on ever placed on their profile and then delete the profile from there to have it completely removed.[25] In early 2009, according to Facebook's user and privacy agreement, once a profile is deleted from Facebook, the site still owns rights to images and profile content stored in their database. Facebook later removed that item from their terms of use and privacy statement after a huge uproar over the issue occurred.[21]

The privacy torts of *intrusion* and *false light* could be used to help control cyber bullying and identity theft online. Intrusion would protect against identity theft and false identities online because the individual has a right to confidentiality concerning private matters and thus would protect against information being gathered by someone into their account or by Facebook allowing for someone to be in an advance search when they have requested not to be searchable. The false light tort would protect against both cyber bullying and false identities on the web because it works against the spread of false, distorted, or misleading information about an individual that would be considered "highly offensive to a reasonable person."

The *appropriation* tort could also have been used in effect with Facebook's policy of owning the right to users' images even after they've terminated their accounts. Because it was in the privacy policy, users could not have used the tort at the time it occurred, because agreeing to the terms of use and privacy policy meant the user gave consent to Facebook to have rights to their profile and pictures. Now that it has been taken out of the privacy policy, however, once could sue if they do use you image or

likeness to their benefit without your consent. The problem, yet again, with privacy tort law, is that if it goes to court, many people have their cases thrown out or lose them due to an inaccurate and limited understanding of privacy law among the courts. [10]

Applicable Case Laws: In February 2010, a class action complaint was filed alleging that Google Inc. broke the law with its Google Buzz service that shared personal data without the consent of users. Google Buzz allows users to post updates, videos, photos and links within its popular e-mail service in a manner similar to Facebook's News Feed. But users' "followers" were pre-selected based on those they frequently e-mail or chat with. Those people automatically see all the other followers, as well as photos and information shared in other Google products like Reader and Picasa. There were concerns that this material aided stalkers, cyber bullying, false identities, and the like.

The legal complaint accused Google of breaking various electronic communications laws, including the Computer Fraud and Abuse Act. Google had turned Gmail "into a social networking service and that's not what they signed up for, Google imposed that on them without getting their consent," said Kimberly Nguyen, consumer privacy counsel with EPIC of Washington, D.C.[31] In November 2010, Google paid an out of court settlement of $8.5 million into a fund for privacy education.[29] The settlement also maintained that Google must do more to educate users about Google Buzz's potential impact on privacy. The $8.5 million from the settlement went towards lawyer fees (30%) and the seven named plaintiffs (up to $2,500 each), with the remainder going towards organizations and non-profits focused on Internet privacy.[30]

Direction of court ruling: Facebook will need to be careful in the future with installing new features into its system like the advance search that overrode people's wishes to not be searchable online or by non-friends and users not in their networks. If Facebook creates the illusion that one is able to basically hide one's profile, then Facebook would be fraudulently appearing to protect user privacy when it is in fact not. The intrusion tort, in this instance, may actually have a good deal of grounds because the users who chose to hide their profiles had a reasonable belief to a right of privacy with their accounts. Facebook users also would have grounds to sue over the false light tort, or could even sue over defamation if they weren't considered some sort of public figure, in the case of fake profiles or hacked in profiles. If a user or person reports defamatory remarks that are offensive to a reasonable person to Facebook and the site doesn't take the profile or remarks down, they that user would have good grounds to sue over defamation or the false light tort if it was malicious in nature (and they were considered some type of public figure, which is more often the case than not when displaying one's profile publicly online).

The appropriation tort could potentially also be successful to sue under for individual users who terminate their accounts, and Facebook still keeps and uses their name and likeness for marketing purposes or otherwise—*if* that statement is retracted from Facebook's user agreement. If it is not taken out of the site's user agreement, then there would be no grounds for users to sue the site on that issue. Based on the results of the Google Buzz class action lawsuit, it would be reasonable to believe that Facebook users could have the same success in suing over changes in the social networking site

that affected user privacy and was not modified in the user agreement and current users weren't asked to review the new agreement and give consent. This is all very hard to judge, however, based on a case settled out of court. Many times large companies decide to settle out of court even if they might have won the case, because they want to get the case over with as soon as possible and move on.

C. Safe for minors?

In October 2007, Facebook started receiving flak over its protection for minors who had accounts on the site. The office of New York Attorney General stepped up its warnings against the social networking site claiming that Facebook would face a consumer fraud charge for misrepresenting how safe the site is for minors. Facebook claimed that its closed-site model made the service safer for minors than other social networks, and that privacy and harassment concerns received prompt responses. However, that was simply not the case since Facebook no longer required the ".edu" email address to sign up, for example. The NY Attorney General's office issued a subpoena for documents from the site, and claimed that investigators posing as young users of the site (12 to 14 years old) were solicited by adult sexual predators numerous times. Facebook was apparently slow or unresponsive in addressing many of the complaints that were lodged as investigators posed as both minors and parents of minors.[26]

The problem is that Facebook, just like any other commercial website, must follow the COPPA guidelines and regulations. In 2004, COPPA fine a site $400,000 for collecting personal information of minors knowingly without parental consent, which is

a hefty fine for a government agency. Facebook's asking minors to provide their age, grade, school, or other information, is a violation of COPPA if they don't receive parental consent first. Facebook must also block information collected from users who are under 13 years old. (The policy is no users under 13: "*No information from children under age 13.* If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us through this help page. *Parental participation.* We strongly recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet and we encourage parents to teach their children about safe internet use practices. Materials to help parents talk to their children about safe internet use can be found on this help page.") Facebook should not have content directed towards children or have statements that would appeal to children, due to possible violation of COPPA. Sites have to be very careful when defining the age of their target audience in lieu of these issues.[7]

The *intrusion* tort, yet again, would be the most probable privacy tort to help regulate Facebook activities for minors. Minors have the right, just as any other user and actually more so, to privacy on the web. There are strict privacy laws concerning minors' information being collected on the web that Facebook should follow, and it should also not misrepresent the safeness of the site for minors. Intrusion would protect against intrusive information gathering practices of Facebook on minors' accounts. Due to the

sensitivity of courts to infractions against minors, the intrusion privacy tort may work better in this case than in others if a suit went to court. [10]

Applicable Case Laws: The settlement with Google paying out $8.5 million for the privacy suit over Google Buzz is an applicable case law for child information protection. In addition, in November 2010, the FTC charged EchoMetrix, Inc., with failing to adequately inform parents using its web monitoring software that information collected about their children would be disclosed to third-party marketers. EchoMetrix sold its Sentry software to parents to allow them to monitor their children's online activities. When Sentry is installed on a computer, parents can log in to their Sentry account and view the activity taking place on the target computer, including chat conversations, instant messaging and the web history.

EchoMetrix also advertised Pulse, a web-based market research software program that it claimed would allow marketers to see "unbiased, unfiltered, anonymous" content from social media websites, blogs, forums, chats and message boards. One source of content available to Pulse users, the FTC alleged, was portions of the online activity of children recorded by the Sentry software. The FTC charged that EchoMetrix violated federal law by failing to adequately disclose to parents, the Sentry subscribers that it would share the information it gathered from their children through the use of its Sentry monitoring program with third-party marketers through Pulse. The only disclosure made to parents about this practice was a vague statement approximately 30 paragraphs into a multi-page end user license agreement. EchoMetrix had to agree not to use or share the information it obtained through its Sentry program

for any purpose other than allowing a registered user to access his or her account. The settlement order also required the company to destroy the information it had transferred from the Sentry program to its Pulse database of marketing information.[36]

Direction of court ruling: Facebook, by requiring that a user must be 13 years of age or older, does cover itself quite a bit with this issue. However, this limit could be ignored by users younger than 13, who lie about their age and thus not need any parental consent to use the site. Thus, Facebook would be obtaining information on those children 13 and under, which is against COPPA. This is an issue that has yet to be dealt with fully, but will most likely play out in courts in the future. It is hard to predict at this point how the courts would rule, since Facebook technically is trying to weed out users younger than 13 with their age restriction, but the argument could be made that Facebook has content appealing to kids under 13 and thus encouraging them to forge their way into the site. The other issue, however, is that users under 18 are legally minors, and thus still need protection from online predators. The fact that Facebook claims it is safe for minors to use, is deceptive in nature, because no user is required to have a ".edu" address (like johndeer@utk.edu) to register with the site anymore. If complaints about online predators are slowly attended to or ignored altogether, then that may also be grounds for a suit over intrusion. Because this deals with minors, courts are more likely to side with the users over the corporate website, regardless of their said privacy policies—i.e. this is something for Facebook to get a tighter hold on unless they want to be faced with some costly lawsuits in the future.

D. Terms of Use and Privacy Agreement (electronic contracts)

In August 2009, five people filed a suit against Facebook charging the company with violating California privacy laws and false advertising. Users assume that personal information and photos that they post on the site are shared only with authorized friends. “Users may be unaware that data they submit ... may be extracted and then shared, stored, licensed or downloaded by other persons or third parties they have not expressly authorized,” the suit read. Writing and photos that people share on the Internet are protected by California law, so using that content without permission from the owner infringes on the creator's rights. The law suit faulted Facebook for collecting and analyzing site content without user knowledge or consent.[21] Another suit, filed in October 2010, claimed Facebook breached its own privacy policy by sharing users’ personal information with advertisers, while another, filed in November 2010, alleged users’ photos to promote "Friend Finder" were appropriated by Facebook without permission. In *In re Facebook Privacy Litigation* (Case No. 10-cv-02389), lawyers for Facebook.com argued the plaintiffs lacked standing, failed to state a claim on which relief could be granted, and neither suffered injury nor damages.[28]

Assessing Facebook’s privacy statement against the FTC’s recommended privacy codes reveals quite a bit behind the controversy of privacy surrounding the social network:

1. *Notice/ Awareness*

Facebook does address the information it will include on the whole with its Privacy Policy, but it does fall short in other areas. It fails to inform account users how their

data will be used, and Facebook says that the targets of potential disclosure are anybody the site deems appropriate (including marketing partners). Facebook has close relationships with several corporations and they integrate their marketing efforts into the site by giving them special “Groups” for interested account users. This disclosure is legal, and users are receiving the use of an extremely useful and popular site for free in exchange for it. However, not all users understand the terms of the bargain: 46% of Facebook users believed that Facebook could not share their information with third parties.

2. *Choice/ Consent*

Facebook does not take sufficient steps to protect user privacy: firms are using it for marketing purposes. As per the usage agreement, a user can request Facebook to not share information with third parties, however, the method of specifying this is not located on the privacy settings page. There is no evidence that one's request is actually honored. The issue at hand then is that there are virtually no controls on what Facebook can expose to advertisers. The blanket statement regarding disclosure allows Facebook to disclose any personal data to advertisers. It also allows advertisers to set cookies that are not governed by the privacy policy.

3. *Access/ Participation*

This feature of the privacy statement is mainly for credit agencies and other organizations which have files on users which they may not want to disclose. Since Facebook is based on the sharing of information, and because Facebook provides

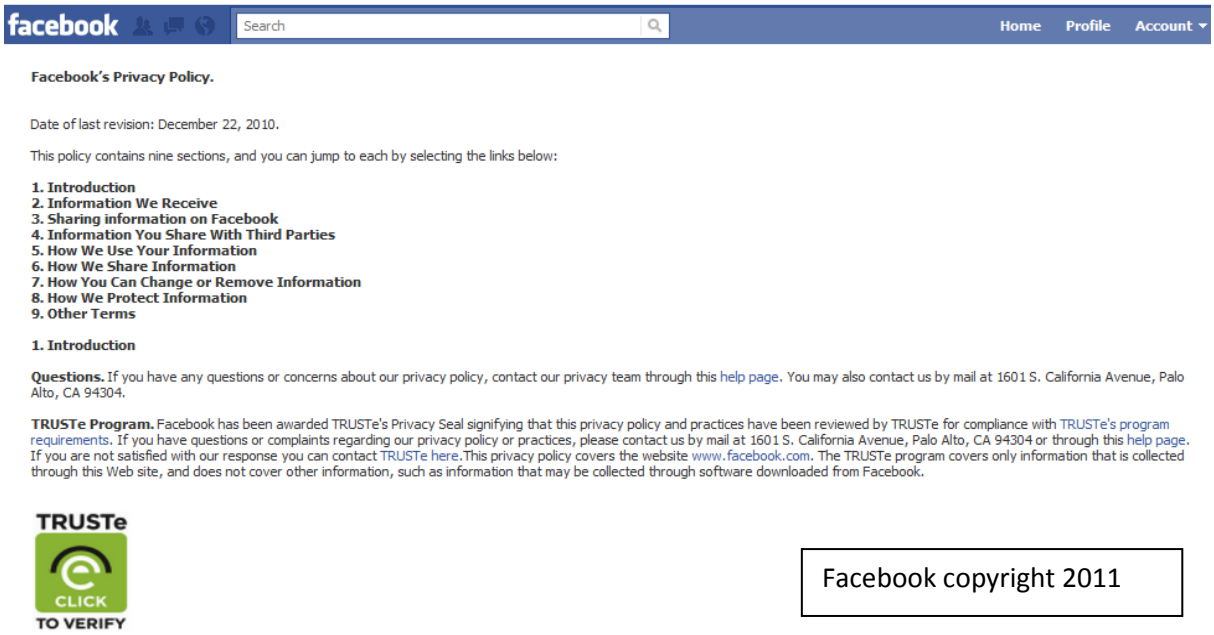
users with the ability to control this information, the social networking site follows this standard reasonably well.

4. *Integrity/ Security*

   By security measures, the FTC considers the ability of encryption in the transmission and storage of data, the use of passwords, and the storage of data on secure servers that are inaccessible by modem. Facebook falls short by FTC standards here. Facebook does use passwords to protect accounts; the site does not use encryption—all authorization information is sent in the clear, even account passwords, making them exceedingly vulnerable on a public network. By today's technology and network standards, it is inferior to the latest password and information protection practices.

5. *Enforcement/ Redress*

   This code requires that customers are aware of ways in which they may be harmed. In the case of a security breach, there is no policy to notify customers if it occurred.[25]


facebook Search Home Profile Account

Facebook's Privacy Policy.

Date of last revision: December 22, 2010.

This policy contains nine sections, and you can jump to each by selecting the links below:

1. Introduction
2. Information We Receive
3. Sharing information on Facebook
4. Information You Share With Third Parties
5. How We Use Your Information
6. How We Share Information
7. How You Can Change or Remove Information
8. How We Protect Information
9. Other Terms

1. Introduction

Questions. If you have any questions or concerns about our privacy policy, contact our privacy team through this help page. You may also contact us by mail at 1601 S. California Avenue, Palo Alto, CA 94304.

TRUSTe Program. Facebook has been awarded TRUSTe's Privacy Seal signifying that this privacy policy and practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements. If you have questions or complaints regarding our privacy policy or practices, please contact us by mail at 1601 S. California Avenue, Palo Alto, CA 94304 or through this help page. If you are not satisfied with our response you can contact TRUSTe here. This privacy policy covers the website www.facebook.com. The TRUSTe program covers only information that is collected through this Web site, and does not cover other information, such as information that may be collected through software downloaded from Facebook.

TRUSTe CLICK TO VERIFY

Facebook copyright 2011

With online contracts, one is legally bound by registering with the site, or by clicking or checking one's agreement with the policy. One's acceptance of the online contract means that, whether one read the policy fully or just scrolled to the bottom, that one now is bound to it and cannot sue for purposes outlined in the policy just because one did not read them.[4] The question then that is brought up is should there be an opt-out option within privacy settings and contract or should that be the default and users decide to opt in? Currently, the default on Facebook's privacy settings is that anyone can view one's profile and the privacy settings are not exactly accessible on the site or easy to navigate through. The default settings are designed to disclose a lot of information with little thought of the consequences.[10]

The two privacy tort laws that would help enforce terms of use and privacy agreements would be *intrusion* and *appropriation*. By going against its own privacy policy, Facebook violated the intrusion tort. Its users had a reasonable belief that their information was to be shared with only those they chose to share it with via their privacy settings. However, Facebook went against its own privacy policy, sharing user information with other entities. Thus the intrusion tort could be used saying that Facebook allowed intrusive information gathering on their users. The appropriation tort would protect against the use of a person's name or likeness for the benefit of another. So when Facebook used users' photos to promote "friend finder" on its site, they violated the appropriation tort, because the social networking site did not get consent from its users to use their images in that specified way. In these cases, since they are

allegedly a violation of Facebook's privacy policy and terms of use, these torts would probably hold up in a court case scenario. [10]

Applicable Case Laws: The settlement with Google paying out $8.5 million for the privacy suit over Google Buzz is an applicable case law dealing with terms of use and privacy policy violations since Google Buzz was added on (much like other Facebook features) after a user agreed to their Gmail account user policies—thus making their profile more public and accessible went against their electronic user contract. This is a case for Facebook to keep in mind as it moves ahead with new ventures.

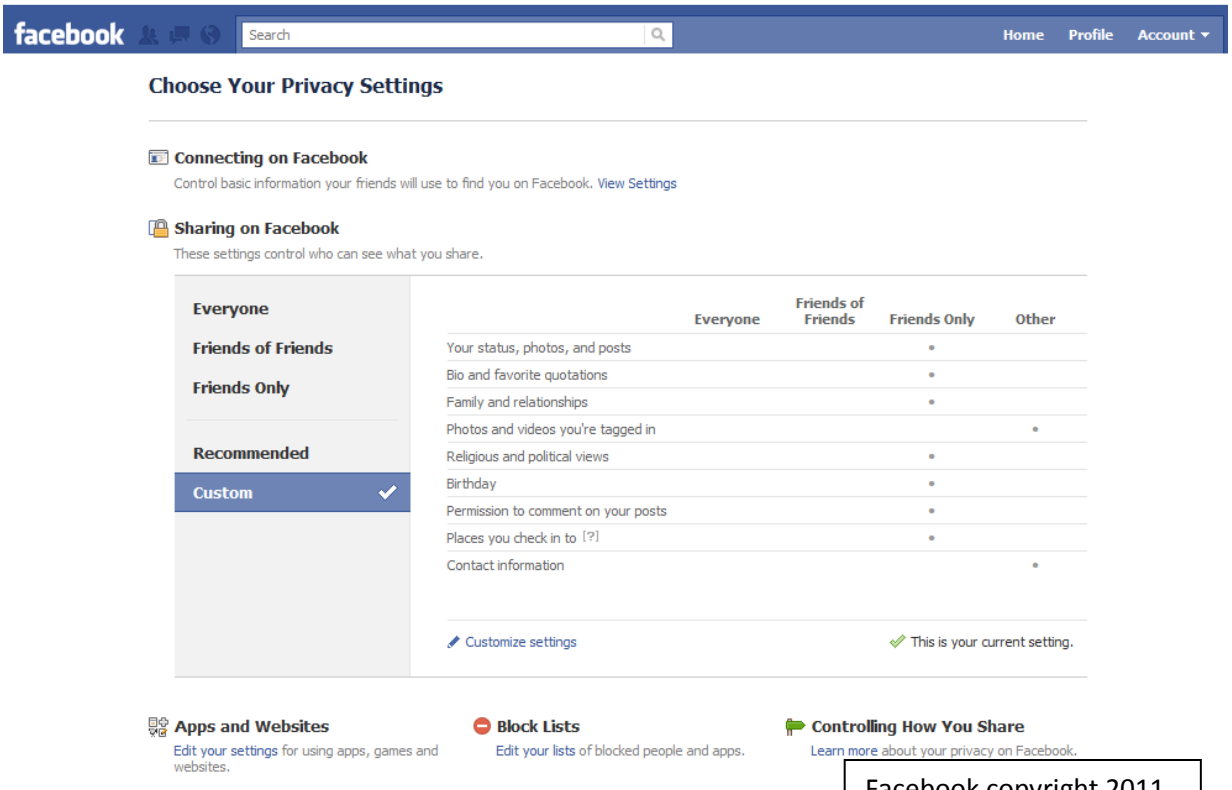
Direction of court ruling: Facebook users, as mentioned before, may be successful in a suit against the social networking site when changing its user policies without at least some sort of notification and/or when just blatantly breaking those agreements. Google had to pay out a hefty settlement for creating Google Buzz and including everyone having a Gmail account—they didn't sign up for Google Buzz, they signed up for email services. This is the same case for Facebook—users didn't sign up for "Friend Finder," they didn't opt into Facebook sharing their information with third party companies. The "Friend Finder" issue may be very successfully be regulated through the appropriation tort—if it wasn't stipulated in the user agreement originally and users weren't notified of the change, then users could sue Facebook under the appropriation tort. Also, if users had a reasonable right to believe they could expect privacy with their accounts because of Facebook's user agreements and privacy policy, and Facebook went against those agreements, users could have grounds to sue Facebook under the intrusion tort.

E. Too much disclosure among users?

In October 2005, Cameron Walker, a then sophomore at Fisher College in Boston, was expelled from the school and barred from the campus. Fisher College expelled Walker because he created a Facebook group supporting the firing of a certain campus security officer thought to regularly overstep his bounds of duty. School officials apparently monitored Facebook and then asked Walker to remove the group. They ultimately canceled his student status. Walker's expulsion could set a precedent for university officials.

Students believe that the information they post on Facebook should be protected, while school officials, especially at schools with strict codes of discipline, will use evidence posted on Facebook to bring formal disciplinary charges against students. This is the first incident of a student being expelled for actions on Facebook. In short, users often disclose too much, and university administrators can now possibly use Facebook for disciplinary purposes.[25] Although some people express concern over privacy, it is not always reflected in their actions. Ninety percent of Facebook users say they have not looked at the privacy policy, while close to 60 percent said they weren't that concerned with privacy and only around 10 percent said that they were very concerned. In one study done by Ralph Gross and Alessandro Acquisti, a researcher requested as a friend hundreds of thousands of Facebook users (i.e. allowing him access to their profile information). Around 30 percent accepted the stranger's friend request. However when Facebook created the "News Feed" and "Mini-News Feed" features in 2006, there was an outcry among Facebook users that it was too "Big-Brother" in

nature. Users viewed this as an invasion of privacy, although only friends could see other friends in their newsfeeds. The problem lies in the idea that users don't expect absolute secrecy or privacy, but they do expect limits on the exposure of their information. Yet, many users don't understand the extensiveness of their exposure online, and many don't grasp the consequences of the breadth of the Internet and placing exposing information online.[10]



Facebook copyright 2011

The *intrusion* tort would be what one could possibly use in such cases stated above. Students have a belief in their right to privacy on the web, and on Facebook, from their administrators. However, if they do not set their privacy settings to where these people cannot see their information or the pages they create, then Facebook ultimately is not at fault for what is set by the user as publicly viewable content. The concern with the "News Feed" also could be covered by intrusion, however, Facebook

claims that only those users who you are friends with would pop up on one's feed and vice versa—thus you could readily access that information by simply going to their page. So unless one is able to view non-friends on one's "News Feed" or a user is showing up on non-friends' feeds, then the intrusion tort is not applicable in these cases.[10]

Applicable Case Laws: In July 2008, a court ruling in Viacom V. Google, established that Google (owner of YouTube) must give Viacom access to what people watched on YouTube. There was large concern over whether Viacom would use the information to track down individual users who watched copyrighted video clips on the site. Viacom made no plans to track down end users, but if it had, it would have been a violation of privacy rights of YouTube's user agreement. Google's IP address statement asserts that "in most cases" the IP address is not identifiable, but not in all cases—meaning that at least some YouTube users are identifiable, and must be protected by the Video Privacy Protection Act (stating that people's choice of videos is very personal and deserved the strongest protection). The login information included "for each instance a video is watched, the unique 'login ID' of the user who watched it, the time when the user started to watch the video, the internet protocol address other devices connected to the internet use to identify the user's computer (IP address), and the identifier for the video."[34] With this court ruling, it appears that the legal tide is changing for user-based websites (YouTube, Flickr, eBay, MySpace, and even Facebook): in the past the courts have been quite clear that if the users violate laws—by posting copyrighted video of Viacom's Comedy Central shows on YouTube, for example—the website isn't liable.

More often now, however, the courts have been siding with owner's rights and ruling that sites are responsible for illegal material posted on their site. Viacom tried to claim that YouTube was encouraging its users in participating in illegal viewing by highlighting copyrighted videos in their "most watched" section. In the future whether user information like Google was court ordered to hand over to Viacom is used to prosecute individual end users could potentially cause a lot of privacy issues and violations.[33]

Direction of court ruling: If Facebook users have set their privacy settings so that their profile is not viewable to the public, then they have an expectation to at least some level of privacy depending on how restrictive they choose to make their privacy settings. If Facebook states in their privacy policy that they will not give information to outside users, and the site does, then it is violating its privacy agreements. Thus if it were to give information out to universities who requested it on their students, Facebook would be in violation of user privacy. However, if universities were able to go onto Facebook on their own and see student profiles or pages, then it is the student's problem for not setting their privacy settings more stringently.

If Facebook was court ordered to hand over information then that can become more complicated, just as with Viacom and Google over YouTube. If a state has subpoenaed information from a corporate website that is incorporated in a different state, there is the issue over whether the site ignores the subpoena or violates its privacy agreement and gives the information to the state court, because that state technically has no authority over the company according to some state laws. In most

cases when the government becomes involved, there is illegal activity that a user is involved with, in which case the courts may not fault Facebook for giving over information. Thus, the site probably would not have much to worry about users suing over court-ordered personal information and winning.

F. Spyware

A security breach on Facebook could potentially put all 8 million plus Facebook records at risk. A security breach could occur from an outsider locating vulnerability using spyware. This is not a risk that can be eliminated, so no site is perfectly secure. Third parties are actively seeking out end-user information using Facebook, and thus intruders are exploiting security holes. The fact that a user's username and password are sent as clear text and not encrypted is a major security vulnerability. Someone could read Facebook user names and passwords off of the Ethernet or unencrypted wireless track, obtain access to users' passwords, as well as any additional accounts they use those passwords for. Facebook should have a policy regarding disclosures of private information due to security breaches or unethical employees. Having a clearly stated requirement in their terms of service that they notify end-users whose privacy was violated would empower and enlighten end-users.[25]

The problem with regulation of these issues is that there is a vast difference among states' regulations and between state and federal regulations. General state prohibitions include:

(1) a person or organization who is not an authorized user may not:

a) modify the computer's homepage, web access provider, or bookmarks

b) collect personally identifiable information by means of keystroke logging function, a program tracking all of a user's behavior, or a program that extracts information from the computer's hard drive

c) prevent the user's efforts to block the installation or disabling of software

d) misrepresent that certain actions on behalf of the user will uninstall or disable undesirable software

e) remove or disable security, antispyware, or antivirus software

(2) a person or organization not authorized may not cause the installation of a software program that:

a) takes control of the computer to spoof email, hijack the computer's modem or Internet service, launch a denial of service attack, or serve a series of pop-up advertisements

b) modifies security settings

c) prevents the user from stopping the installation or disabling of computer software

(3) a person or organization not authorized may not induce a user to install software onto the user's computer:

a) by falsely representing that the software is necessary for security purposes or in order to view specific content

b) in order to get the user to violate other prohibitions of the spyware legislation.

The problem with state laws is that there are vast differences among them, making it hard to regulate online when the website entity is in another state that the user who

has been violated by spyware. Some states require that spyware actions be intentionally deceptive to be prosecuted, while others just require that the action be deceptive. People who can enforce the statutes range from only the state attorney general in Arkansas to any party or person who had been violated by spyware. The amount in which the states penalize spyware practices range from $100 in Georgia to $100,000 in Arizona. There are also federal proposals made by the House and Senate that are similar to the state laws, but they also vary quite a bit in enforcement, penalties, and preemption.[7] Spyware and security flaws in corporate websites cause data breaches quite often, disclosing personal information. And many state laws now enforce these businesses to notify users of the breach when it occurs. The FTC is also requiring that all personally identifying and private information be encrypted—something that Facebook has yet to comply with.[7]

Intrusion and *disclosure of private facts* torts could be used to regulate spyware issues. Intrusion would protect again third party spyware seeking to break into Facebook information systems and individual accounts; because all users have a right to believe that their information is safe from third parties not listed in Facebook's privacy agreement. Disclosure of private facts would cover the issue of Facebook's lack of security against spyware systems, in which case one could sue Facebook for ignorance (i.e. not encrypting its information), and thus disclosing private user information.[10]

Applicable Case Laws: In December 2010, a second suit was brought against Apple. It claimed that "personal, private information was obtained without their knowledge or consent ... their personal property—their computer—was hijacked by said

defendants and turned into a device capable of spying on their every online move." Similar to the previous suit against Apple mentioned in this paper, this suit also claims that the apps could personally identify the users through the phone's UDID, which cannot be changed, as well as other data gathered from user activity.[37] In January 2011, a civil suit was filed in U.S. District Court in New York, where a plaintiff was seeking class action status for allegations of inappropriate activities known as "browser sniffing" and "flash cookie" abuse. The suit asked the court to make Interclick delete personal information and give plaintiffs profits made from use of the data. Interclick's browser sniffing is based on several non-transparent functions according to the suit: Interclick embedded a history searching code invisible to the consumer within its code which displayed an advertisement and then eventually the history searching code would transmit the findings of this to Interclick's servers. The suit also alleged that Interclick was able to take advantage of "cookie respawning." Deleting HTTP cookies to prevent tracking can be thwarted through "respawning." The Flash cookie value would be rewritten in the standard HTTP cookie value, thus undermining the user's attempt to prevent tracking. HTTP cookie respawning is on several sites, including About.com, Hulu.com, Answers.com, Aol.com, and Mapquest.com.[38]

Direction of court ruling: Facebook users would have a good chance of suing under the intrusion and disclosure of private facts torts, if there was in fact spyware, like with Interclick, on Facebook's site (which there have at this point been no allegations of such, it has just been a speculated concern). Users could expect a payback amount for money made off of the spyware as well from Facebook—as was the case with Interclick.

Facebook, because it has neglected to encrypt its login information, has made the site and individual user information more vulnerable than necessary. The courts maybe would make Facebook inform users of a security breach and pay fees for damages to individual users caused by Facebook's lack of security.

V. Suggestions

A. What should the law do?

The law works best when it can be a lingering threat in the backdrop, but still allows most problems to be worked out informally. Law suits are threats to keep people in check, without them people would be invading one another's privacy without any regard. The issue, however, is to have a lawsuit be a realistic threat without being brought undeservedly. In our current legal system, we do have solutions to privacy issues online, but they are extremely limited in their effectiveness.[10]

The problem with expanding the range of legal privacy protection is that it might encourage more lawsuits. However, if the law makes it too hard to sue, then the law ceases to be a credible threat at all. So the issue is maintaining the law as a plausible threat, but at the same time keeping unnecessary and frivolous law suits in check. [10]

The easiest route to this would be to require a plaintiff to exhaust all informal methods of dealing with the privacy issue or violation. Then if the defendant agrees to remove the harmful information from the website or to stop the violation of privacy, then this should ideally be the end of the lawsuit—unless the plaintiff demonstrates that merely taking down the information or cease and desisting won't sufficiently repair

the damage. The next step would then be that the plaintiff must prove that he attempted to seek informal redress, but the defendant did not adequately comply before a lawsuit can occur. Or the plaintiff must prove irreparable damage (i.e. it has gone viral), even if the defendant has then removed the harmful information or stopped the privacy violation.

Another solution would be to create incentives for partied to go through a mediator or arbitrator rather than through court: mediation being non-binding, and arbitration being binding. These "alternative dispute resolutions" could possibly cut down a considerable amount of legal costs and could resolve issues quicker. Another way to cut down on legal expenses is to reduce the amount of damages that can be claimed in a lawsuit. The threat of massive damages hinders free speech, thus limiting damages would encourage free speech. Limiting damages would not serve to minimize those who have been harmed by defamatory statements or privacy violations, and there of course should be exceptions for extreme cases or cases that show a pattern of abuse. The law should be there to impart some responsibility on those who post online and online companies and deter the spread of falsities and invasions of privacy. [10]

B. Ways to achieve the right balance of law:

1. Refurbishing the Appropriation Tort

The closest privacy law that comes to the powerful law of copyright is the appropriation tort. It prevents the use of someone else's name or likeness for financial benefit. The tort has developed in such a way that it is often fairly ineffective in protecting privacy rights. It originally was set forth in order to protect a

person's privacy, but it is now used as more of a property right. The courts had previously declared that the use of a person's identity was like stealing his liberty, temporarily putting him under the control of another, with the effect that the person was then no longer free and was virtually a slave. Over time, the tort lost that meaning. It is now limited mainly to instances where a person's identity is exploited for commercial gain. The tort is not applicable to the use of someone's name or likeness by the news, in art, in literature, etc. So, when writing about the person, their image is free game—as long as no money is made off of it. The appropriation tort could be expanded to cover a larger range of issues surrounding privacy invasion. Possibly, that could mean that the appropriation tort applies when people's photos are used in any way that is not of legitimate public concern.[10]

The other three torts (intrusion, public disclosure of private facts, and false light) are better suited at this point to cross-over into privacy protection on the web. Although, they most certainly could be strengthened by mentioning the Internet as a medium along with other media that are already regulated and stated specifically in the Restatement of Torts.

2. State laws and regulations

State efforts to protect personal privacy are limited by what is deemed constitutionally permissible. The Commerce Clause of the US Constitution does not favor state efforts to control interstate commerce or commercial conduct occurring outside a state's borders. Fraudulent and criminal activity on the Internet seems to be reachable by state action, but otherwise legal conduct on the Internet seems to

be out of state legislation's reach. The Internet has no boundaries—least of all state boundaries. Thus most of state regulation of the Internet would affect not just intrastate commerce, but actions occurring out of state and even outside of the US. So for state legislation to be able to regulate the Internet there would need to be an undisputed expansion of state authority into territories outside of the state itself. Another issue is that more than one state can enact legislation, bringing about inconsistent and irreconcilable regulations among states. State legislation that aims to control privacy on the Internet will most certainly be deemed unconstitutional if it doesn't take these matters into consideration.[6]

Illinois, for example, enacted a law that prohibited the advertisement of controlled substances (even FDA approved medications) by name; however, it was struck down because it was impossible to run a national ad campaign via the Internet without violating the statute. Illinois' law had overstepped its boundaries because it would be impossible to prevent state residents from accessing the drug's website or block the state from national advertising broadcasts. On the other hand, a Texas statute prevented car manufacturers from competing with licensed dealers by selling used cars to Texas consumers over the Internet was upheld. This is because the state's law didn't require termination of say Ford Motor Company's website—Ford simply continued promoting their used cars and just said the offer was void where prohibited by law.[6] Utah enacted legislation in 2003 that prohibited the installation of spyware on another's computer that monitored the computer's usage. The bill required "plain language" licensing agreements in order to obtain

user's consent to spyware or adware. This statute was maintained and thus spyware programs had to inquire whether the user was from Utah in order proceed with trying to install itself on the user's computer.[7]

Thus, the main problem with state laws regulating the Internet is not that multiple states might regulate a given transaction, but rather how the regulating state is selected. Businesses can protect themselves by abiding by the most rigorous state law that a court may apply. The court could go in two directions—the state where the Internet company is incorporated or the state in which the violation of privacy occurred in (i.e. the residence of the individual whose privacy was violated). Internet jurisdiction has gone through three phases. Initially, a state could exercise jurisdiction on the basis that the website was broadcast into the state. Next, courts based jurisdiction on the level of activity of the website in that particular state. Courts now are even siding with websites over states' jurisdictions when the site can prove it was targeting a certain state or targeted its conduct elsewhere.[12]

In 2010, a set of potential class actions were filed in Fulton County, Ga., Superior Court against three Internet powerhouses addressing the government's ability to see what people do on the Web, but the bigger issue was how Georgia subpoenas and warrants were served and where they were actually valid. The suits claimed that Comcast, Yahoo and Windstream violated federal wiretap and computer privacy laws by providing information in response to warrants or subpoenas issued by Georgia judges or magistrates, which are then faxed or otherwise relayed to the Internet companies' headquarters outside of Georgia. If they had been federal

warrants, there would be no issue, but they were state warrants and the suits claim that those warrants have no force outside the state of Georgia. However, in Yahoo's user policy statement, it says that they will share information if "We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities." The Internet companies may also be able to use their presences in every state as a defense. This is yet another example of issues concerning state regulation of the web and Internet privacy concerns.[32]

State regulation of the Internet appears to be the pioneering frontier of privacy law, and it will work best for the time being for three main reasons. For one, Internet companies can pick and choose where they want to be incorporated and thus which state's laws they want to be under. State residents can also choose whether or not they like their state's policies and elect new government leaders if they do not, or worse case scenario—move to a different state. Thus people and companies can control state regulation to an extent and squelch inefficient rules or laws. Second, because of the vast number of approaches to and levels of protection the states can take, state regulation may result in an equilibrium in which different states' laws appeal to different Internet companies. Finally, providing states with the opportunity to develop their own Internet regulations, allows for the experimentation and evolution of the law, which then will shed some light on the best approach. Mandating a federal law too soon would discourage state regulation and experimentation, and the government may not find the best way to regulate the Internet.[12]

State privacy laws differ greatly from state to state. Data breach notification laws, for example, are part of a broader effort to address identity theft and the security of personal information data. In some states, the notification laws create private causes of action, while others restrict enforcement to the attorney general's office. Currently there are as many approaches to data breach notification as there are laws, and the number of approaches is likely to grow as more states enact these laws. There are eight states that do not even have any data breach notification legislation, and there are around ten other states that don't have specific data breach laws but have considered it in past years.[7]

Delaware, where Facebook is incorporated, has the most lenient laws regulating corporations. Any individual or company conducting business in the state that owns or licenses computerized data must disclose a breach of security of any resident whose unencrypted information was or is believed to have been acquired by an unauthorized person. The entity or person who maintains the data must inform the owner or licensee of the information as well. If notice is required, written notification must also be provided to the Consumer Protection Division of the Department of Justice. A business that maintains its own notification procedures and is consistent with the statute's timing procedures is deemed in compliance as long as the correct people are notified. A Delaware resident is entitled to recover damages, and if damages are awarded the person can get triple the amount of actual damage plus attorney fees. The Attorney General can also commence an action for damages or injunctive relief.[7]

Tennessee has similar data breach laws to Delaware as far as who is covered by them, the information protected, and when the breach notification is required. However, the means of notification are much different. For one, if a person must notify more than 1,000 people at one time, then they must also notify all consumer reporting agencies and credit bureaus. The manner must be written, email or telephone, unless the it will cost more than $250,000, or over 500,000 people must be notified, or the business does not have contact information, then there must be a substitute notice which must include all of the following: email notice, posting on the website, notice to statewide media, and notification to major statewide media. The owner of the information that was breached must also me notified immediately. In Delaware, the laws state that notification of those whose information was given out must be notified without unreasonable delay—which can be quite ambiguous depending on whose opinion is determining the extent of "unreasonable." Delaware's laws also say that owners of the information and the Consumer Protection Division must be notified at some point in time—it doesn't say specifically when as does Tennessee's laws (i.e. "immediately). Entitlement to damages is also different: any customer of an information holder (a person or business, but not a state agency) that is injured by a violation may recover damages through a civil suit (but the amount of damages to which one can receive is not established thus one could get a lot more in damages than in Delaware or significantly less depending on the impact of the breach).[7]

3. Federal laws and regulations

With the case of the Internet, its digital technology makes information borderless across all nations. The Internet is accessible in more than 200 countries worldwide, and online data moves with ease in between them. Instead of enacting a multinational agreement, national or more often time's state and provincial law have been applied to an inherently global medium. This is a huge issue, how does the US create national legislation that controls an international medium?[12]

The US has taken a wait and see approach in favor of industry self-regulation concerning Internet privacy policy making online. The federal government has tended toward marketplace solutions, only using legislation as a last resort. Privacy advocates, however, argue that the industry response has been inadequate and without stronger government regulations, privacy initiatives will not be achieved.[1]

Some arguments have been brought up questioning the effectiveness of state regulation, and thus calling for stronger federal regulations instead. States tend to over regulate because of the ambiguity of jurisdiction and conflicting laws give states substantially more reach than they should have. Contractual choice of law helps somewhat with this; however, state courts may have a tendency to override those contractual agreements in favor of state laws. [12]

The best solution seems to be let state laws prevail for now, so that the federal government can sit back and see what works and what doesn't. It would be counterproductive at this point to heavily regulate emerging technologies with federal law without first allowing states to experiment, compete, and evolve their

laws to discover the right approach or a mix of approaches that work. Then the federal government can make national privacy laws that will be effective and not overreaching but not under regulated either. Hopefully at that point in the future, the US government's privacy and Internet regulations can coincide with international agreements with multiple countries on Internet and privacy regulations. [12]

4. Self regulation

Internet firms are not going to cheat customers because they have strong reputational incentives not to.[12] Online organizations have to balance how far they can go with user information technically, legally, and ethically. Various industries have formed coalitions and associations devoted to online privacy protection in order to gain consumer trust. The Online Privacy Alliance, for example, is a group of 50 Internet companies that abide by the privacy policies of the alliance. TRUSTe provides a third-party "trustmark" seal which allows websites to inform their users of their gathering and information practices as well as provides them with a dispute resolution mechanism (http://www.truste.org/).[1]

It is the responsibility of individual organizations to secure data at rest and data in motion through risk assessments that look at wireless and web transactions. Online organizations must also come up with preventive measures such as penetration testing, intrusion prevention and encryption to better protect user privacy. Organizations who advertise online must also make it a priority to know

what happens to the data that is collected, especially if a third party provider is involved.[35]

Along with posting privacy policies entailing how data is collected, used, and disclosed, websites have been using some specific strategies to limit the use of data and ensure accuracy. Cookie prompts, opt-in and opt-out features, and incentives like free online services in exchange for consumer data are all some of the approaches websites are now using in self-regulation.[1]

A major question with self-regulation is whether sites should have consumes opt-in to privacy protection or opt-out. For example, a website may be prohibited from collecting information from its users unless it obtains a consumer's agreement (opting-in) to the information gathering, or on the other hand, only if the consumer opts-out of information gathering strategies of a website must the online company cease data collection. An opt-in procedure draws the consumer's attention to his or her right to refuse consent, whereas an opt-out strategy reduces the directness of which the consumer is presented an explicit choice.[12]

5. Consumer awareness

Many consumers are resorting to their own self-help strategies, along with a few software programs that appear to be helping with consumer privacy. Anti-spam software filters and encryption software like PGP (Pretty Good Privacy), as well as anonymous remailers and "anonymizers" (which strip away personally identifying information) all give consumers control over their personal data. There is also Platform for Privacy Preferences (P3P) and Trustlabels which allow consumers to

determine the privacy policies of a particular website and choose whether or not to interact with that site's cookies. The P3P lets users select their privacy preferences and warns the user if a site falls outside of that. Trustlabels prompt users to accept or reject individual cookies whose privacy settings fall outside the user's preferences. All of these technologies provide consumers with greater control over their information and privacy and allows users to assume a more active role in protecting their information.[1]

The Electronic Privacy Information Center has come up with "11 Things You Can do in an Hour to Protect Your Privacy":

1. Opt out of prescreened offers of credit: call 1-888-567-8688 or visit https://www.optoutprescreen.com/.
2. Stop your phone records from being sold: call landline and wireless phone companies and request to opt-out of "CPNI" sharing. CPNI is your call records information—most phone companies sell lists of the calls you make and receive.
3. Keep your banking records private: under federal law, your bank can sell your account information, including your bank balances, unless you direct them not to. Call all banks that you use and ask to opt out from all information sharing.
4. Get free credit monitoring: all Americans are entitled to a free credit report from each of the three nationwide consumer reporting agencies. You can perform a free form of credit monitoring by requesting one of your three credit reports every four months. Visit https://www.annualcreditreport.com or call 1-877-322-8228.

5. Do-not-Call Registry: enroll your phone numbers (landline and wireless) in the FTC anti-telemarketing list by calling 1-888-382-1222.
6. Safeguard your SSN: the Social Security number is the key to identity databases. Those who have it can steal your identity and engage in fraud. Do not keep your SS Card or any other document that contains your SSN in your wallet. Also, don't give out your SSN unless it is in a tax or employment context.
7. End student profiling: children's schools can sell personal information to marketers and military recruiters. Federal law allows you to opt out of this profiling.
8. Avoid loyalty programs: supermarket and other loyalty cards track your purchases and make it easier for companies to sell your information. You can ask for a new loyalty card every time you go, switch with a friend every so often, or just not use one.
9. Secure your accounts: be sure to place a password on your banking, phone, and utilities accounts. A password makes it more difficult for others to access your records.
10. Turn off third party cookies: turn off third party cookies, and only accept cookies that are first party or from the originating website. This makes it more difficult for profilers to track you online.
11. Engage in privacy self defense: don't give your phone number or other personal details to businesses unless they really need it. Be sure to ask businesses how they use your personal information, whether they sell it, and how they protect it.

> Don't complete product warranty cards, surveys, or sweepstakes—they are just ways to collect and sell your data.[8]

VI. Summary and Conclusions

In conclusion, privacy law has evolved immensely over the years since its inception in the very beginnings of the United States. However, privacy law still has a ways to go to become more effective regulating the new medium of the Internet. The four privacy torts have great potential to control the Internet without being too over regulative, but they either need to be reworked to apply to the Internet or it must be added in a new Restatement of Torts. The US has taken an approach of waiting to see what issues arise before making federal laws to control the Internet, and at that they have only made laws that cover certain sectors of commerce—FTCA, COPPA, Gramm-Leach-Bliley Act, Fair Credit Reporting Act, and HIPAA. This is not necessarily a negative thing, because it has allowed states to make their own privacy laws concerning the Internet and they have been able to see what works best for what situations. The Internet, however, is still very new, and it will be quite a while before federal legislation would be an appropriate step forward in Internet privacy regulation because the states are still experimenting with their laws.

There are three main issues with privacy and trust over the Internet: visibility, accountability, and scale. A lot of what happens on the Internet is basically invisible. When ISPs, websites, or third parties collect data, that activity is usually hidden from the provider of that data. Second, when data travels from one computer to another or is combined with other data, information instructing how the data should be or not be used is not included. Data doesn't

have a tag on it saying which user agreement policies the provider consented to. If people or companies use the data in a way not agreed upon, there is usually no one who is automatically accountable. Third, the Internet connects people and organizations that can be hard to identify and from all parts of the world—the scale of the information sharing is intimidating.[11]

Facebook, although hit with a lot of privacy suits recently, is more or less doing the best it can under the current ambiguity of privacy laws or merely lack thereof altogether. Many of the issues the social network has been sued over haven't had clear cut laws to back up the suits. Many times Facebook has settled out of court, not out of fear for losing, but wanting to keep their customers happy and to move on from the issue. Every time there has been a major complaint about a privacy feature, Facebook has moved to correct the issue, even if what they were doing was not illegal—it wants to keep its users happy, and it wants to grow. Are there things which Facebook can do better?—most certainly. In the eye of the law, however, Facebook has done nothing illegal thus far. It has set forward a user agreement and privacy policy that users must agree to before receiving a Facebook account—so if users have an account, they have agreed to the privacy policy whether they like it or not. If current privacy laws change or tighten up, then Facebook may have to edit some of its current practices, but for the time being the company is probably safe.

The future of Internet privacy law is somewhat uncertain at the moment. For now, it appears the federal government will take a back seat to state government regulation, at least until it sees what is the best way to regulate the borderless medium. There may possibly be a blanket federal privacy law in which states can enact stricter versions if they so choose. Or the

federal government may band together with other countries and create a multinational law that will better regulate the Internet—but that takes an agreement on what aspects of privacy are valued among those countries involved. Right now, the Internet is providing services to consumers for their information. Facebook, for example, is providing users with a free social networking site. In return, users can provide as little as basic demographic information to their likes, interests, and activities, which is all valuable information to marketers who want to pay Facebook to place their ads on the target consumer's page.[13] Facebook, along with several other Internet sites and even other technological mediums such as TiVo, provide users with a sense of "consumer control" which normalizes the surveillance in their own homes, and allows markets to further examine the user and sell their products. Users are getting paid for this work they are doing, however, so each individual has to decide for themselves whether they think their newfound control has enough equity for them. Many argue that surveillance and invasion of privacy should be reframed from "the disappearance of privacy" to "a shift in control over personal information from individuals to private corporations."[2] Consumers get something in return for their information. Ultimately, it is the consumer's responsibility to be informed and know what he or she is doing on the web. They have to read the privacy policies, not just scroll though them without reading and check the "I accept" box. They have to take some responsibility to protect their own information.

So, how much legal protection does the average consumer get on the Internet and how much does the consumer actually need? There is stringent legal protection on specific privacy issues on the Internet; however, overall, the Internet has very little controls except for the self-regulation that websites place on themselves through user agreements and privacy policies.

The average consumer does need more protection, but privacy regulation of the Internet is still in its infancy and will take time and experimentation to figure out the right amount of control.

Bibliography

Journals and Hard Copy:

[1] Albarran, Alan B. and David H. Goff, eds. Understanding the Web: Social, Political, and Economic Dimensions of the Internet. Ames: Iowa State University Press (2000).

[2] Andrejevic, Mark. The work of being watched: Interactive media and the exploitation of self-disclosure. *Critical Studies in Media Communication*, 19(2), 230-248 (2002).

[3] Ballon, Ian, J. Brelsford, and S. Levi, eds. Third Annual Internet Law Institute (Volume I). New York: Practising Law Institute (1999).

[4] Ballon, Ian, J. Brelsford, and S. Levi, eds. Third Annual Internet Law Institute (Volume II). New York: Practising Law Institute (1999).

[5] Bowrey, Kathy. Law and Internet Cultures. New York: Cambridge University Press (2005).

[6] Frackman, Andrew, R. Martin, and C. Ray, eds. Internet and Online Privacy: A Legal and Business Guide. New York: ALM Publishing (2002).

[7] Gilbert, Francoise, et al. eds. Seventh Annual Institute on Privacy Law: Evolving Laws and Practices in a Security-Driven World (Volume I). New York: Practising Law Institute (2006).

[8] Gilbert, Francoise, et al. eds. Seventh Annual Institute on Privacy Law: Evolving Laws and Practices in a Security-Driven World (Volume II). New York: Practising Law Institute (2006).

[9] Goldsmith, Jack and Tim Wu. Who Controls the Internet?: Illusions of a Borderless World. New York: Oxford University Press (2006).

[10] Solove, Daniel J. The Future of Reputation: Gossip, Rumor, and Privacy on the Internet. New Haven: Yale University Press (2007).

[11] Stefik, Mark. The Internet Edge: Social, Legal, and Technological Challenges for a Networked World. Cambridge: The MIT Press (1999).

[12] Thierer, Adam and Clyde W. Crews Jr., eds. Who Rules the Net?: Internet Governance and Jurisdiction. Washington D.C.: The CATO Institute (2003).

[13] Van Dijck, Jose. Users like you? Theorizing agency in user generated content. *Media, Culture, and Society* 31(1), 41-58 (2009).

[14] Warren, Jim, J. Thorwaldson, and B. Koball, eds. Computers, Freedom, and Privacy. Los Alamitos: IEEE Computer Society Press (1991).

Websites:

AOL

[15] Berlind, David. ZDNet. On heels of AOL's privacy snafu, is a class action lawsuit next? (Aug. 9, 2006). <http://www.zdnet.com/blog/btl/on-heels-of-aols-privacy-snafu-is-a-class-action- lawsuit-next/3460> (viewed Feb. 6, 2011).

[16] Lawyers and Settlements: America's Premier Online Legal News Source. AOL Privacy Class Action Can Proceed: California Residents Can sue AOL in California (Jan. 20, 2009). <http://www.lawyersand settlements.com/case/aol-privacy-class-action-can-proceed-time-warner.html> (viewed Feb. 6, 2011).

[17] Mark, Roy. Internet.com: ISP Planet. AOL Loses Subscriber Privacy Suit (Nov. 6,2002).<http://www.isp-planet.com/news/2002/aol_021106.html> (viewed Feb. 6, 2011).

Facebook

[18] Calderón, Sara Inés. Inside Facebook: Tracking Facebook and the Facebook Platform for Developers and Marketers. Facebook Roundup: Canada, Privacy, Yahoo, Ads, Lawsuits and the NBA (May 29, 2010). <http://www.insidefacebook.com/2010/05/29/facebook-roundup-canada-privacy-yahoo-ads-lawsuits-and-the-nba/> (viewed Nov. 2, 2010).

[19] Davis, Wendy. MediaPost Blogs. Facebook: Privacy Suit Fails To Specify Injuries (July 19, 2010). <http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid =132270> (viewed Feb. 6, 2011).

[20] Gaudin, Sharon. Computer World. Lawmakers hit Facebook CEO with privacy questions (Oct. 19, 2010). <http://www.computerworld.com/s/article/9191818/Lawmakers_hit_ Facebook_CEO with_privacy_questions> (viewed Nov. 2, 2010).

[21] Gohring, Nancy. PC World: Tech Industry. Facebook Hit With Privacy-Violation Lawsuit (Aug. 18, 2009). <http://www.pcworld.com/article/170402/facebook_hit_with_privacy violation_lawsuit.html> (viewed Nov. 2, 2010).

[22] Internet.com: eSecurity Planet. Privacy Lawsuits Target Facebook, Google, Zynga (Nov. 1, 2010). <http:// www.esecurityplanet.com/headlines/article.php/3910791/Privacy-Lawsuits-Target-Facebook-Google-Zynga.htm> (viewed Feb. 6, 2011).

[23] Johnson, Bobbie. Guardian.co.uk: Technology Blog. How Facebook tried to put a shine on $9.5m privacy suit (Sept. 21, 2009). <http://www.guardian.co.uk/technology/blog

/2009/sep/21/facebook-privacy> (viewed Nov. 2, 2010).

[24] Jones, Ashby. The Wall Street Journal: Law Blog. Facebook Poked with New Privacy Lawsuits (Oct. 20, 2010). <http://blogs.wsj.com/law/2010/10/20/facebook-poked-with-new-privacy-lawsuits/> (viewed Nov. 2, 2010).

[25] Jones, Harvey and José Hiram Soltren. Facebook: Threats to Privacy (Dec. 14, 2005). <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf> (viewed Nov. 2, 2010).

[26] McCarthy, Caroline. CNET News. Facebook's legal issues escalate as N.Y. attorney general strengthens warnings (Oct. 1, 2007). <http://news.cnet.com/8301-13577_3-9788413-36.html> (viewed Nov. 2, 2010).

[27] Mills, Courtney. WebProNews: Breaking eBusiness and Search News. Facebook Privacy Issues Getting Worse (May 25, 2010). <http://www.webpronews.com/blogtalk/2010/05/25/facebook-privacy-issues-getting-worse> (viewed Nov. 2, 2010).

[28] Toplitt, Sheldon. The Unruly of Law. Facebook Seeks to Dismiss Class-Action Privacy Suits (Jan. 17, 2011). <http://theunrulyoflaw.blogspot.com/2011/01/facebook-seeks-to-dismiss-class- action.html> (viewed Feb. 6, 2011).

Google

[29] Kang, Cecilia. Washington Post: Post Tech. Google settles Buzz privacy suit, tells users by e-mail (Nov. 2, 2010). <http://voices.washingtonpost.com/posttech/2010/11/google_on_tuesday_said_it.html> (viewed Feb. 6, 2011).

[30] Parr, Ben. Mashable. Google Settles Buzz Privacy Lawsuit for $8.5 Million (Sept. 3, 2010). <http://mashable.com/2010/09/03/google-buzz-lawsuit-settlement/> (viewed Feb. 6, 2011).

[31] Temple, James. The San Francisco Chronicle: SFGate. Local class action complaint filed over Google Buzz (Feb. 17, 2010). <http://www.sfgate.com/cgi-bin/blogs/ techchron/detail?entry_id=57438> (viewed Feb. 6, 2011).

Yahoo

[32] Land, Greg. Yahoo Finance: Law.com, the Fulton County Daily Report. Internet Privacy Suits Filed Against Yahoo, Others (Oct. 7, 2010). <http://finance.yahoo.com/news/Internet-Privacy-Suits-Filed-law-804555832.html?x=0> (viewed Feb. 6, 2011).
(Full article found at Law.com: <http://www.allvoices.com/s/event6954939/aHR0cDovL2Mub W9yZW92ZXIuY29tL2NsaWNrL2hlcmUucGw/cjMyNDg1NDE3MTYmYW1wO3c9MjM5MDUxMg= =>)

You Tube

[33] Holahan, Catherine. Bloomberg Business Week. Viacom vs. YouTube: Beyond Privacy (July 3, 2008). <http://www.businessweek.com/technology/content/jul2008/tc2008073_435740.htm> (viewed Feb. 6, 2011).

[34] Opsahl, Kurt. Electronic Frontier Foundation. Court Ruling Will Expose Viewing Habits of YouTube Users (July 2, 2008). <http://www.eff.org/deeplinks/2008/07/court-ruling-will-expose-viewing-habits-youtube-us> (viewed Feb. 6, 2011).

More

[35] Blount, Gail. PRLog: Free Press Release. Privacy Lawsuits Increase in 2010 Due to Online Behavioral Tracking (Jan. 25, 2011). <http://www.prlog.org/11248685-privacy-lawsuits-increase-in-2010-due-to-online-behavioral-tracking.html> (viewed Feb. 6, 2011).

[36] Bureau for Consumer Protection Business Center: FTC. Legal Resources. <http://www.ftc.gov/privacy/ privacyinitiatives/promises_enf.html> and < http://ftc.gov/os/caselist/1023006/101130 echometrixcmpt.pdf >(viewed Feb. 6, 2011).

[37] Elgan, Mike. Internet.com: Datamation. Why Privacy Lawsuits against Apple Matter to Google (Dec. 29, 2010). <http://itmanagement.earthweb.com/secu/article.php/3918786/Why-Privacy-Lawsuits-against-Apple-Matter-to-Google.htm> (viewed Feb. 6, 2011).

[38] Springer, Paul. Trader Daily. Flashing, Respawning Cookies Lead to Privacy Suits (Jan. 5, 2011). <http://www.traderdaily.com/01/flashing-and-respawning-cookies-lead-to-privacy-suits/> (viewed Feb. 6, 2011).

[39] Zeran vs. AOL (97-1523). United States Court of Appeals for the Fourth District. Brief of Appellant (Apr. 23, 1997). <http://legal.web.aol.com/decisions/dldefam/zeran appellant.pdf> (viewed Apr. 10, 2011).

Case Laws:

AOL

Google

Yahoo

YouTube

Apple

EchoMetrix

Interclick